Tenable EOL Release Notes

Last Updated: May 30, 2025

Copyright © 2025 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Tenable EOL Release Notes

Use the following list to view end-of-life (EOL) Tenable product release notes.

- Tenable Identity Exposure
- Tenable Log Correlation Engine
- Tenable Nessus
- Tenable Agent
- Tenable Network Monitor
- OT Security
- Tenable Security Center

Tenable Identity Exposure Release Notes

To view EOL Tenable Identity Exposure release notes, see Tenable EOL Release Notes.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

View the following Tenable Identity Exposure (formerly Tenable.ad) release notes:

Tenable Identity Exposure 3.19 On-Premises (2022-04-20)

[On-prem]

New Features

- **Scalability** — Dynamic activation and deactivation of Indicators of Exposure.
- **LDAP authentication** — The ability to enable/disable SASL bindings. For more information, see Authentication using LDAP in the Tenable Identity Exposure Administrator Guide.
- **Memory cache** — Tenable Identity Exposurehas greatly improved its memory consumption to benefit Indicators of Attack (IoAs).
- **New Indicators of Attack** (For more information, see the Tenable Identity Exposure Indicators of Attack Reference Guide.)
    - **DPAPI Domain Backup Key Extraction** Indicator of Attack can detect a wide variety of attack tools that use LSA RPC calls to access backup keys.
    - **Massive Computers Reconnaissance**: Detects reconnaissance attacks that generate a massive number of authentication requests to Active Directory targets.
    - **Enumeration of Local Administrators**: Detects Active Directory data enumeration attacks.

    - **NTDS Extraction**: NTDS exfiltration refers to the technique that attackers use to retrieve the NTDS.dit database that stores Active Directory secrets such as password hashes and Kerberos keys.

    - **SAM Name Impersonation**: This Indicator of Attack detects an attacker who tries to exploit two vulnerabilities that can lead to an elevation of privileges on the domain from a standard account without any security skills.

    - **Kerberoasting** IoA to detect and alert to Kerberoasting attacks targeting Active Directory service account credentials.

- **Windows Server 2022** — On-premise support for Windows Server 2022.

- **Retirement of the Caroli component** — Retired to optimize platform performance.

- **Retirement of InfluxDB & Equuleus** — Retired to optimize platform performance and data consistency.

    > **Note**: For on-premises installations, the change in Tenable Identity Exposure's database implementation will cause the loss of historical data in the dashboards during upgrade. On-premises platforms will lose the history of statistics in the User, Deviances, and Compliance Score. Widgets for Users/Deviance count and Compliance Score will recover their most recent values after reinitialization; however, line chart widgets will only have one data point and will recover their values progressively.

- **Domain connectivity tests** — Allows you to test a domain connectivity (LDAP and SYSVOL) before you add or modify it.

- **Scalability** — Tenable Identity Exposure considers resolved deviances as no longer useful and clears them from the database after 6 months.

- **Indicator of Exposure** — Improvements to the Indicator of Exposure **Logon restrictions for privileged users**.

- **Workload quota** — New ability to adjust the limit on the number of Indicators of Attack running simultaneously.

- **Attack Path**: New graphical representations to explore Active Directory relationships:

    - **Blast Radius**: Evaluates lateral movements in the AD from a potentially compromised asset.

- **Attack Path**: Anticipates privilege escalation techniques to reach an asset from a specific entry point.
- **Asset Exposure**: Measures an asset's vulnerability using asset exposure visualization and tackles all escalation paths.

- **Honey Accounts** — Allows the Kerberoasting Indicator of Attack to detect login or service requests. For more information, see Honey Accounts in the *Tenable Identity Exposure Administrator Guide*.
- **API Endpoint** — Retrieval of Active Directory objects from the database using the API.
- Tenable Identity Exposure propagates changes — such as a move or rename — on an LDAP container to the container children.

Bug Fixes

In addition to performance improvements, Tenable Identity Exposure version 3.19 contains the following bug fixes:

Bug Fix	Defect ID
Tenable Identity Exposure returns the API Score information again.	N/A
The widget edition now takes into account previously selected domains.	N/A
Tenable Identity Exposure now provides better analytics performances thanks to new SQL index.	N/A
Tenable Identity Exposure displays attacks that occur on the 1st day of the month in the correct month.	N/A
When you remove a GPO, Tenable Identity Exposure only displays the deleted event.	N/A
When the SYSVOL connection breaks, Tenable Identity Exposure renews the connection to allow the listener to fetch new events.	N/A
The allow lists for Credentials Roaming users and groups now accept the `samAccountName` format.	N/A
Tenable Identity Exposure considers resolved deviances as no longer useful and	N/A

clears them from the database after 6 months.	
Tenable Identity Exposure now counts users with an unknown `userAccountControl` attribute as active AD users. This can happen when the account provided in Tenable Identity Exposure does not have the right to read this attribute or a corresponding attribute set. This can lead to an increase in the total number of users in the dashboard or the license. For more information, see User Accounts in the Technical Prerequisites document.	N/A
Tenable Identity Exposure propagates changes — such as a move or rename — on an LDAP container to the container children.	N/A
Connection to the SYSVOL share succeeds even if you change the credentials.	N/A
Kerberos dangerous delegation now resolves after privileged path is corrected by deleting and recreating the domain.	N/A
The whitelist now clearly specifies the expected format.	N/A
The SQL server functions correctly after Attack Path activation.	N/A
The notification email contains the correct image format.	N/A
Control Path relations now consider the source and target type.	N/A
Tenable Identity Exposure updates the children DN when it detects when a container move.	N/A
It is no longer possible to delete the last user with an administrative role using the public API.	N/A
Indicator of Exposure (IoE) `C-PKI-DANG-ACCESS`: • Deviances no longer appear and disappear. • Takes into account the IoE's allow list.	N/A
The C-DC-ACCESS-CONSISTENCY IoE takes into account the "Keep deleted DCs" toggle update.	N/A
The IoA/IoE service restarts after a toggle update.	N/A

The `C-PASSWORD-POLICY` IoE now allows all non-global security groups.	N/A
Tenable Identity Exposure limits dashboard names to 30 characters and truncates existing names exceeding this limit to 30 characters.	N/A
Tenable Identity Exposure stabilized the retrieval of AD objects from the SQL server when it encounters a low number of objects with many changes.	N/A
The Dangerous Delegation RBCD Backdoor now resolves the account SID.	N/A
Tenable Identity Exposure does not keep attempting to process large messages.	N/A
Native administrative group members IoE (`C-NATIVE-ADM-GROUP-MEMBERS`): Placing built-in administrative groups in the custom group option no longer creates inconsistent behaviors.	N/A
The Logon restrictions for privileged users IoE (`C-ADMIN-RESTRICT-AUTH`) now resolves when you remove a computer from a sub-organizational unit.	N/A
The `Sleeping Accounts` IoE no longer counts deleted users.	N/A
The Tenable Identity Exposure API now sends a 400 error when there is no active provided at user creation.	N/A
Tenable Identity Exposure now supports Windows LTS versions.	N/A
Deleted sites no longer appear in deviances.	N/A
Tenable Identity Exposure updates group members when they change OUs.	N/A
When the Active Directory is slow, the regular crawling no longer starts if a crawling is already in progress.	N/A
Migration from 3.1 to 3.11 does not generate false positives deviances on GPOs.	N/A
The Tenable Identity Exposure crawling phase supports more edge cases.	N/A
Tenable Identity Exposure's on-premise installer now ensures that it uses up-to-date NodeJs modules.	N/A
Tenable Identity Exposure's analytics service successfully reconnects to the RabbitMQ server after failures.	N/A

The partial recrawling of `groupPolicyContainers` objects takes all attributes into account.	N/A

Patches

Tenable Identity Exposure 3.19.12

Tenable Identity Exposure version 3.19.12 contains the following patches.

Patch	Defect ID
Fixed CVE-2022-37026 by upgrading the RabbitMQ library dependency.	N/A
Windows Server 2022 — The server no longer needs to reboot when installing Indicators of Attack on a Windows 2022 Domain Controller.	N/A

Tenable Identity Exposure 3.19.10

Tenable Identity Exposure version 3.19.10 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure no longer collects the AD attribute `msds-revealedusers` and no longer shows it in the Trail Flow. It was not useful in the security analysis.	N/A
The RabbitMq channel connection improved in resiliency.	N/A
In IoE page, filtering one given domain no more shows unexpected compliant "No Domain" IoEs.	N/A

Tenable Identity Exposure 3.19.9

Tenable Identity Exposure version 3.19.9 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure no longer does the Server Authentication EKU check on the SecProbe.	N/A
On partially-domain-joined machines, Tenable Identity Exposure now successfully	N/A

decodes any SDDL bi-grams related to the domain (e.g. DA for Domain Admins).	
The IoE **Dangerous sensitive privileges** is correct when an *AdObjectGptTmpl* object that disables the UAC comes last.	N/A

Tenable Identity Exposure 3.19.8

Tenable Identity Exposure version 3.19.8 contains the following patches.

Patch	Defect ID
The crawling and listening of the SYSVOL use the same connection so that they no longer collide.	N/A

Tenable Identity Exposure 3.19.7

Tenable Identity Exposure version 3.19.7 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure improved the efficiency of the internal message consumption.	N/A
Tenable Identity Exposure improved the RabbitMQ channel connection resiliency.	N/A
Tenable Identity Exposure no longer collects the `userCertificate` attribute.	N/A
RabbitMQ consumers now keep retrying to connect on an exclusive queue.	N/A
The Indicator of Attack *Enumeration of Local Administrators* IoA now filters out the enumeration of local admins when done locally as this is most likely a legitimate action.	N/A
Tenable Identity Exposure automatically resolves deviances related to a removed domain or security profile in internal calls.	N/A
The installer now takes into account the locale when checking the expiration date of custom certificates.	N/A

Tenable Identity Exposure 3.19.5

Tenable Identity Exposure version 3.19.5 removed the **Ransomware Hardening** Indicator of Exposure due to a premature release.

Tenable Identity Exposure 3.19.4 (on-premises)

Tenable Identity Exposure version 3.19.4 contains the following patches.

Patch	Defect ID
The PDF export of the IoAs' consolidated view is available for on-premises installations.	N/A

Tenable Identity Exposure 3.19.2 (on-premises)

Tenable Identity Exposure version 3.19.2 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure displays the domain details of the topology view with the new time-series data.	N/A
The Tenable Identity Exposure installer can handle regional date/times (on-premises).	N/A

Tenable Identity Exposure 3.19.1

Tenable Identity Exposure version 3.19.1 contains the following patches.

Patch	Defect ID
Indicators of Exposure use again a thread-safe hashing cache.	N/A
Tenable Identity Exposure removes old multi-valued attributes efficiently without blocking the database.	N/A

Tenable Identity Exposure 3.11 — On-premise & SaaS (2021-12-01)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features (SaaS)

Tenable Identity Exposure version 3.11 includes the following new features:

- A new indicator of exposure lists dangerous permissions and misconfigured parameters related to the Windows Public Key Infrastructure (PKI).

New Features (dedicated for on-premises)

- Secure communications between components via TLS using Tenable Identity Exposure's self-signed auto-generated certificate or a custom certificate.
- A dedicated MSI for the security probe installation.

New Features (on-premises, previously available for SaaS)

- A lockout policy to mitigate brute force attacks against authentication mechanisms. It aims to lock out user accounts after too many failed login attempts.
- A product licensing feature to allow you to update your Tenable.ad license.
- Ability to disable certain indicators of exposure without restarting the security engine node.
- Support for the localization process.
- Single domain recrawling to force the refreshing of data for a domain.
- Use of native Server Message Block (SMB) mapping.
- Upgrade of Node.js to v16.

Bug Fixes

Tenable Identity Exposure version 3.11 contains the following bug fixes:

Bug Fix	Defect ID
Tenable Identity Exposure purges the previous version's events from internal queues after each upgrade.	N/A
The analytics service successfully reconnects to the RabbitMQ server after failures.	N/A
The indicator of exposure C-PASSWORD-POLICY is more resilient against a specific corner case.	N/A
Tenable Identity Exposure ignores InheritOnly ACEs when it checks ACLs to avoid	N/A

false positives.	
The trail flow no longer freezes.	N/A
The indicators of attack requiring Sysmon tolerate better versions of Windows event, which strengthens detection.	N/A

Patches

Tenable Identity Exposure 3.11.8 (2022-09-19)

Tenable Identity Exposure version 3.11.8 contains the following patches.

Patch	Defect ID
When a Storage Manager upgrade fails, it is possible to do a rollback.	N/A
The OpenSSL upgrade covers all dependencies.	N/A

Tenable Identity Exposure 3.11.7 (2022-04-06)

Tenable.ad version 3.11.7 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure correctly flushes out Login event (4624) from its cache memory after a Logoff event (4634).	N/A
Tenable Identity Exposure displays attacks that occur on the 1st day of the month in the correct month.	N/A
When you remove a GPO, Tenable Identity Exposure only displays the deleted event.	N/A
When the SYSVOL connection breaks, Tenable Identity Exposure renews the connection to allow the listener to fetch new events.	N/A
The allow lists for **Credentials Roaming users and groups** now accept the `samAccountName` format.	N/A

This patch also updates OpenSSL-related software to address the security issue CVE-2022-0778.

Tenable Identity Exposure 3.11.6 (2022-03-08)

Tenable.ad version 3.11.6 contains the following patches.

Patch	Defect ID
SQL services are running when upgrading from version 3.11.3.	N/A
Split architecture installations include TLS options.	N/A
Rabbit MQ correctly resumes after upgrading from version 3.1.5 to 3.11.3.	N/A
Event insertion no longer affects performance.	N/A
Events for Indicators of Attack do not consume too many memory resources.	N/A

Tenable Identity Exposure 3.11.5 (2022-02-09)

Tenable Identity Exposure version 3.11.5 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure deduplicates Windows event logs' strings to reduce memory usage.	N/A

Tenable Identity Exposure 3.11.4 (2022-01-24)

Tenable Identity Exposure version 3.11.4 contains the following patches.

Patch	Defect ID
The Tenable Identity Exposure installer pre-fills values for IP/ports from variables during an upgrade.	N/A
The upgrade correctly considers existing certificates.	N/A
The SQL service account can now access local certificates.	N/A
Tenable Identity Exposure updates group members when they change Organizational Units (OU).	N/A
The Security Probe installer completes after a reinstallation.	N/A
The Tenable Identity Exposure installer verifies that the PFX certificates are valid.	N/A

Tenable Identity Exposure 3.1 - On-prem and SaaS (2021-07-28)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features and Improvements

Tenable Identity Exposure version 3.1 includes the following new features and improvements:

- Indicators of Attacks detect live security incidents that impact your AD infrastructure.
- The Setup View enables you to configure quickly the attack detection in selected domains.
- The Consolidated View lists the security incidents detected on the monitored infrastructures over time.
- The Investigation View displays the incident timeline of a specific resource.
- New checker: codename C-GPO-EXEC-SANITY.
- Query history in the Trail Flow View.
- Query bookmarks in the Trail Flow View.
- Improved database storage.
- Password encryption in clear text.

Bug Fixes

Tenable Identity Exposure version 3.1.0 includes the following bug fixes.

Bug Fix	Defect ID
The checker no longer raises a deviance for the NETWORK SERVICE account's "Replace a Process Level Token" privilege.	N/A
Tenable Identity Exposure takes into account the allow list option.	N/A
Tenable Identity Exposure resolves dynamically the "The LAPS GPO does not exist" problem.	N/A
Tenable Identity Exposure resolves the deviance in an XML file when the related	N/A

file is deleted.	
An "Unlinked GPO" deviance is no longer triggered when the option "Extract unlinked GPOs" is deactivated.	N/A
Tenable Identity Exposure now supports the infinite lockout duration GPO parameter.	N/A
Checkers are now correctly processed when running a full recheck after an initial check.	N/A
Icons on the far right no longer blur out a long search query in the Trail Flow.	N/A
It is now possible to customize an IoE with a long list of parameters.	N/A
Tenable Identity Exposure replicates displayed data when copying a deviant element in the event details.	N/A
Tenable Identity Exposure distinguishes the system-assigned domain name from the domain FQDN in all checkers.	N/A
The dashboard display can support over 80 configured domains without freezing.	N/A
Tenable Identity Exposure now resolves all well-known SIDs.	N/A
In role creation, you can select "create" permissions and deselect "modify" permissions in the same section.	N/A
The role description now supports unicode characters seamlessly.	N/A
Tenable Identity Exposure now applies the correct new user role if that role had been changed.	N/A
Tenable Identity Exposure takes into account Security Principals when it computes deviances.	N/A
Crawlers can now connect to the customer's Active Directory.	N/A
The SYSVOL parser supports UTF-8-encoded files with a BOM header.	N/A
The SYSVOL crawler now can run multiple instances in parallel.	N/A
Adding too many CIDR in Ceti's networks no longer prevents connection to the	N/A

Active Directory.	
Refresh Topology batch no longer over-consumes resources.	N/A
Tenable Identity Exposure displays two distinct trust relationships even if they start from and end at the same domain.	N/A
Tenable Identity Exposure redirects the user from the email's "IoE details" and "IoA details" buttons to their corresponding page.	N/A
Tenable Identity Exposure reconnects to the LDAP server when it loses the connection due to an LDAP_SERVER_DOWN error.	N/A

Patches

Tenable Identity Exposure 3.1.10 (2021-12-08)

Tenable Identity Exposure version 3.1.10 contains the following patch.

Patch	Defect ID
Tenable Identity Exposure's crawling phase supports more edge cases.	N/A

Tenable Identity Exposure 3.1.9 (2021-10-12)

Tenable Identity Exposure version 3.1.9 contains the following patches.

Patch	Defect ID
Crawling succeeds even when LDAP requests take a long time to initialize.	N/A
The Sysvol crawling completes successfully despite network errors.	N/A
The fetching of attribute names no longer fails due to timeout.	N/A

Tenable Identity Exposure 3.1.8 (2021-09-27)

Tenable Identity Exposure version 3.1.8 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure can list all previous attacks in a domain's attack	N/A

timeline.	
Tenable Identity Exposure detects password spraying attacks.	N/A
The Sysvol crawling completes correctly even when there are special characters in the file.	N/A
Golden Ticket attack detection does not produce false positives when it receives too many events.	N/A
Tenable Identity Exposure parses correctly the Indicator of Attack file.	N/A

Tenable Identity Exposure 3.1.6 (2021-09-07)

Tenable Identity Exposure version 3.1.6 contains the following patches.

Patch	Defect ID
The Sysvol crawling continues even if the registry.pol file exceeds a given size.	N/A
The LDAP initialization succeeds despite crawling an object without attribute change.	N/A

Tenable Identity Exposure 3.1.5 (2021-08-26)

Tenable Identity Exposure version 3.1.5 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure raises an "NTLMv1 protocol not disabled" deviance when the GPO is unlinked.	N/A
The license lock works with the NFR license.	N/A
The LDAP initialization succeeds despite crawling unreachable groups or excluded objects.	N/A

Tenable Identity Exposure 3.1.4 (2021-08-23)

Tenable Identity Exposure version 3.1.4 contains the following patches.

Patch	Defect ID

The checker now ignores the KRBTGT account.	N/A
Tenable Identity Exposure includes default profile options in any profile.	N/A

Tenable Identity Exposure 3.1.3 (2021-07-28)

Tenable Identity Exposure version 3.1.3 contains the following patches.

Patch	Defect ID
Tenable Identity Exposure displays two distinct trust relationships even if they start from and end at the same domain.	N/A
Tenable Identity Exposure redirects the user from the email's "IoE details" and "IoA details" buttons to their corresponding page.	N/A
Tenable Identity Exposure reconnects to the LDAP server when the connection is lost due to an LDAP_SERVER_DOWN error.	N/A

Tenable Identity Exposure 3.1.0 (2021-06-30)

Tenable Identity Exposure version 3.1.0 contains the following patches.

Patch	Defect ID
The checker now ignores the KRBTGT account.	N/A
Default profile options are included in any profile.	N/A
Tenable Identity Exposure raises an "NTLMv1 protocol not disabled" deviance when the GPO is unlinked.	N/A
The license lock works with the NFR license.	N/A
The LDAP initialization completes even when it attempts to crawl inaccessible objects.	N/A
LDAP initialization succeeds even when it crawls an object that does not have an attribute change.	N/A
The Sysvol Crawler now completes even if the registry.pol file exceeds a given size.	N/A

Tenable Log Correlation Engine Release Notes

To view EOL Tenable Log Correlation Engine release notes, see Tenable EOL Release Notes.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

View the following Tenable Log Correlation Engine (formerly LCE) release notes:

2022 Log Correlation Engine

Tenable Log Correlation Engine 6.0.10 Release Notes (03-17-2022)

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** If you are upgrading from any version earlier than 6.0.0, upgrade directly to 6.0.10. See Upgrade Notes for detailed information about supported upgrade paths.

New Features

- Now also available for OEL8 / RHEL8 / CentOS8.
- New scripts under `/opt/lce/tools/pg-helper-sql/`:
    - `all-columns--decl-order.sql  [<table name fragment>]`
        - Useful when specifying PostgreSQL statistics objects.
    - `planner-estimates.sql <table name> [<mCommonestValues>,=10]`
    - `progress--analyze.sql  [<refreshInterval_seconds>,=15]`
    - `progress--bulk-load.sql  [<refreshInterval_seconds>,=5]`
        - Useful for performance tuning of the `lced` daemon's [a] persisting of events to activeDb, and [b] saving silo snapshots into archiveDb.
    - `progress--stream-backup.sql [<refreshInterval_seconds>,=60]`
    - `rawlog-storage.sql  <silo#>  <percent of rows to scan>`
    - `table-buffer-cache-stats.sql [<table name fragment>]`
- New shell function `list-helper-SQL-scripts-with-usage`, which becomes available in a shell session after you have once run `source /opt/lce/tools/exigent-sessions.bashrc` in that session; it lists the name and usage banner of every helper `.sql` script bundled and invocable with `psqlf` or `psqli`, as explained in the *Tenable Log Correlation Engine User Guide*.
- New action `--recompress` now afforded by the `archival-manager` utility; this retroactively changes the gzip compression level of the constituent files of an archived snapshot in the original location.
- Additional optional arguments, `-<N_newest>` and `<N_oldest>` are now accepted by the `archival-manager` utility's `--list-snapshots` action.
- Additional counters tracked by the `lce_queryd` daemon let you quickly identify `showids` command (encoded query sent from Tenable Security Center) problem areas:
    - The `riskSlow` group, counting queries which likely take significant time to evaluate.
    - The `foreknow_noSuch` group, counting queries which could never return any results.
- The `diag` utility now takes an optional `--sanitize` argument. If this is given, the diagnostics report produced will have overwritten the following: IPv4 addresses, MAC addresses, CPU

serial numbers, chassis serial numbers, and motherboard serial numbers.

- New sections in `diag` report:
  - `operational-logs/querying-profile.txt`
    - For each query received by Log Correlation Engine in the most recent few months, prints a line with:
      - response latency in seconds, or `timed_out`
      - abbreviated name of Tenable Security Center tool
      - query time span
      - traffic direction
      - whether this was an “archive-peek” query
      - which predicates were used.
    - Because lines are formatted consistently, this report is easy to analyze with standard UNIX utilties, a scripting language, or a spreadsheet program.
  - `operational-logs/rawlog-queries-distribution.txt`
    - Reports how many times, in the most recent few months, has Log Correlation Engine received a query containing a particular `+text` filter (in other words, a rawlog predicate). Since such queries are often among the slowest to execute, changing them to filter instead by normalized attributes can significantly improve your Tenable Security Center Events Analysis experience.
  - `ssl_config.txt`
    - Lists the names and sizes of SSL credential files found, grouped by containing directory.
- New sub-sections in `diag` report:
  - In the `clients.txt` section, *“Nonunique sensors”*.
  - In the `disk__space_inodes_mounts.txt` section, *“LVM: physical volumes ... volume groups ... logical volumes”*.

- SSL credentials for Web UI may now be rotated independently of SSL credentials for vuln reporter proxy: the former with `lce_crypto_utils --generate-creds-webUI`, and the latter with `lce_crypto_utils --generate-creds-vulnReporter`.

Changed Functionality and Performance Enhancements

- Underlying datastore upgraded from PostgreSQL 12.1 to PostgreSQL 14.1; as result, Log Correlation Engine realizes the following benefits:
    - Reduced event persistence overhead, due to faster compression of long rawlog strings and to improved performance of binary-mode `COPY FROM`.
    - Less disk needed per silo, due to more space-efficient storage of duplicate entries in BTree-type indexes on low-cardinality columns. (The `upgr6010-partial-reindex-silos` utility will rebuild indexes on silos created prior to upgrade, so you can take advantage of this improvement retroactively.)
    - Improved querying performance in many scenarios.
    - Less interference with daemons' operation by the `optimize-datastore` utility, due to `VACUUM` command operation being now parallelizable.
- Speedup of up to 9%, subject to available host computing resources, of:
    - Saving of silo snapshots into archiveDb by the `lced` daemon.
    - All "archive-peek" operations by the `queryd` daemon.
- The `queryd` daemon now recognizes and removes the " mark that Tenable Security Center occasionally appends to the `showids` queries it sends to Log Correlation Engine, resulting in an illegal query which Log Correlation Engine used to (rightly) reject. This is a workaround for a Tenable Security Center bug.
- The `queryd` daemon now recognizes and removes the `“+event *_* +event *-*”` filter sequence that Tenable Security Center frequently inserts into the `showids` queries it send to Log Correlation Engine, resulting in gratuitous use of computer resources and a needless slowdown. This is a workaround for a Tenable Security Center bug.
- Added the "inverse meepfile" optimization to `queryd` daemon; when applicable, this makes IP address filters smaller and hence conducive to more efficient evaluation.

- Added the "inline specification of IP address filters" optimization to `queryd` daemon; this lets PostgreSQL take advantage more often of indexes on `src_ip` and/or `dst_ip` columns, with resultant query execution speedup.
- To prevent transition into an invalid configuration when adding or editing a client assignment rule, Log Correlation Engine now checks, for every policy *P* mentioned in said rule, that *P* exists and has been successfully loaded.
- To prevent transition into an invalid configuration when adding or editing the `include_networks` or `exclude_networks` configuration attribute, Log Correlation Engine now checks that no `include_networks` subnet overlaps with an `exclude_networks` subnet and vice versa.
- To prevent transition into an invalid configuration when deleting a policy *P*, Log Correlation Engine now checks that *P* is not referenced by any client assignment rules.
- The `make_cert` utility has been removed, and its functionality moved into `lce_crypto_utils`.
- Renamed scripts under `/opt/lce/tools/pg-helper-sql/`:
    - `progress--index-or-reindex.sql`, previously `command-progress--index--create-or-rebuild.sql`
    - `progress--rebuild-table.sql`, previously `command-progress--cluster.sql`
    - `progress--vacuum.sql`, previously `command-progress--vacuum.sql`
    - `planner-estimates--silo.sql`, previously `planner-estimate-basis.sql`

Bug Fixes

- The `lced` daemon could enter dynamic halt during silo roll.
- The `lced` could fail to complete a silo roll; in such a scenario, `lced` would continue to persist events to the last-added silo, but would not perform subsequent silo rolls, trim activeDb as needed, or trim archiveDb as needed.
- The `tasld` and `statsd` daemons could enter dynamic halt if either began working on a silo *S*, and *S* was aged out of activeDb before the daemon in question finished working on *S*.

- The lced daemon could fail to persist updated client activity counters, such as how many events received in the current day or exactly when had an event been last received.
- The RPM installer/upgrader did not halt optimize-datastore process if one was running.
- The diag utility did not correctly report disk space statistics for the filesystem containing a site's archiveDb, if said filesystem was a network mount.
- The lced daemon, in certain rare cases at high-volume site, would fail to persist a minute fraction of events accepted just prior to silo roll.
- Authorization of encrypted syslog senders via the crypt_syslog__authorized_fingerprints configuration attribute did not work in some cases.
- In some cases, archival peek status would not be properly carried across reboots of the queryd daemon.
- An Log Correlation Engine client's IP address and/or sensor name would not be updated in the Log Correlation Engine Server database immediately after the IP address of the client's host changed due to a DHCP re-assignment; the desired update would only happen after a disconnect/reconnect sequence.
- License activation and plugins update failing after January 2022, due to heightened SSL protocol level requirements.
- The queryd daemon would fail to generate response to a showids command requesting some attributes of every event in specified timerange (without any rollup or summarization), if no response size limit had been specified.
- An instance of showids launched by Tenable Security Center could fail to exit while holding on to a PostgreSQL connection; if this happened often enough, PostgreSQL connections would be exhausted, and no utilities would function normally.
- In some cases, the cfg-utils utility, when issued a command with an invalid argument, would emit an error message stating that PostgreSQL datastore is unavailable.
- The --set-sv action of the cfg-utils utility, when used to set activeDb_max_on_disk_size__MB or archiveDb_max_on_disk_size__MB configuration attribute, would interpret its numeric argument as denoting bytes instead of megabytes.
- Credential files produced by the lce_crypto_utils utility did not allow for browser access.

Security Enhancements

- Updated to OpenSSL 1.1.1l
- Prevent a Cross-site Scripting (XSS) vulnerability in the DataTables plugin.
- Prevent an arbitrary code injection via the template function in Underscore plugin.
- Prevent jQuery-UI from executing untrusted code.
- Prevent Regular Expression Denial of Service (ReDoS) in CodeMirror plugin.
- Prevent Remote Code Execution (RCE) in Handlebars compiler on templates coming from an untrusted source.

Upgrade Notes

- If you are upgrading from a version earlier than Log Correlation Engine 4.8.4, upgrade to Log Correlation Engine 4.8.4 before upgrading to Log Correlation Engine 6.0.10.
- If you are upgrading from Log Correlation Engine 5.0.x, upgrade to Log Correlation Engine 5.1.1 before upgrading to Log Correlation Engine 6.0.10.
- If you are upgrading from Log Correlation Engine 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *Tenable Log Correlation Engine User Guide*.
- If you are upgrading from 6.0.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.5 or Later in the *Tenable Log Correlation Engine User Guide*.
- If you are upgrading from Log Correlation Engine 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.10-el6.x86_64.rpm
  ```

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, or 6.0.5, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr606-rebuild-hhourlies &
  ```

> **Note:** The `upgr606-rebuild-hhourlies` script takes approximately 2.5 minutes to run per activeDb silo.

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr603-rebuild-silos &
  ```

  This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

  > **Note:** If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, run `/opt/lce/tmp/upgr606-rebuild-hhourlies` first, then `upgr603-rebuild-silos`.

- If you are upgrading from Log Correlation Engine 4.8.4, 5.1.1, 6.0, 6.0.1, 6.0.2, or 6.0.3, you may be prompted to run `/opt/lce/tmp/restore_per-client_decisions.sql` when the upgrade utility completes. If you receive this prompt and you performed explicit client authorizations (without the aid of client assignment rules or the auto-authorization setting) or specified custom sensor names for individual Log Correlation Engine clients, run:

  ```
  source /opt/lce/tools/source-for-psql-shortcuts.sh
  psqlf /opt/lce/tmp/restore_per-client_decisions.sql
  ```

  This script applies the changes you made to your upgraded Log Correlation Engine.

  > **Note:** If you did not perform explicit client authorizations or specify custom sensor names for individual Log Correlation Engine clients, you do not need to run `/opt/lce/tmp/restore_per-client_decisions.sql`

- (Optional) If you are upgrading from Log Correlation Engine 6.0.0-6.0.9, after the `rpm` command completes, run the following command to recover disk space:

  ```
  sleep 5h ; nohup /opt/lce/tmp/upgr6010-partial-reindex-silos &
  ```

  > **Note:** This script may require up to 20 minutes per activeDb silo to run.

> **Note:** If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, run `/opt/lce/tmp/upgr606-rebuild-hhourlies` first, then `upgr603-rebuild-silos`, then `upgr6010-partial-reindex-silos`.

> **Note:** If you are upgrading from Log Correlation Engine 6.0.3, 6.0.4, or 6.0.4, run `/opt/lce/tmp/upgr606-rebuild-hhourlies` first, then `upgr6010-partial-reindex-silos`.

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit
- Red Hat Enterprise Linux 8 64-bit / Oracle Enterprise Linux 8 64-bit

2021 Tenable Log Correlation Engine

Tenable Log Correlation Engine 6.0.9 Release Notes (06-02-2021)

Tenable Log Correlation Engine 6.0.8 Release Notes (01-21-2021)

Tenable Log Correlation Engine 6.0.7 Release Notes (01-19-2021)

Tenable Log Correlation Engine 6.0.9 Release Notes (06-02-2021)

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** If you are upgrading from any version earlier than 6.0.0, upgrade directly to 6.0.x. See Upgrade Notes for detailed information about supported upgrade paths.

New Features

- New configuration `attribute web_UI__login__client_CA_cert_path` (string type), replacing `webserver__login_requires_client_cert` (Boolean type).
- Additional configuration attribute validation:

- check that {`cloud_vuln_upload__IP_or_FQDN custom_plugins_provider__IP_or_FQDN DNS_cache__domains_to_not_resolve`

  `DNS_cache__FQDNs_to_resolve_greedily`} do not contain any characters illegal in a FQDN or domain name, and that neither '`.`' nor '`-`' is first or last character;
- check that all characters in `exclude_users` and the "sensor" field of {`syslog_sensors intrusion_detect_sensors`} are ASCII, printable, and not whitespace;
- ensure that {`debug minimum_trace_level syslog_message_terminator_characters crypt_syslog__authorized_fingerprints`} can be assigned only values legal for respective attribute.

- Added `check-client-policies`, a utility script that checks for several common errors (malformatted paths, illegal MD5 hashes, etc.) in `.lcp` files. This script may be invoked anytime from console, after you have sourced `/opt/lce/tools/exigent-sessions.bashrc` in that session. It is also invoked by `diag`, with output going to the `policies.txt` section of `diag` report.
- New `filesystem_proc_filehandles.txt` section in `diag` report, to help diagnose inter-application disk contention issues.
- Additional actions now afforded by the `lce_crypto_utils utility`:
  - `--print-privkey`
  - `--print-PKCS12`
  - `--save-as-PKCS12`

Changed Functionality and Performance Enhancements

- The `rebuild_logs` utility has been moved to under `/opt/lce/tools/` for a more consistent deployment directory structure.
- The `diag` utility now gathers more per-process and per-thread info; in particular, cumulative delay due to block I/O waits is now reported.
- Revised mutex locking scheme in the `lced` daemon's event persistence module, to reduce lock contention and therefore inter-core communication overhead.

- Previously, server-side SSL credentials for uploading vulnerability reports toTenable Security Center and for securing interaction with Log Correlation Engine Web UI were shared. This arrangement has been problematic, insofar as the act of rotating credentials used for the one purpose would invariably break the other. Now, while server-side SSL credentials for uploading vulnerability reports to Tenable Security Center remain in `/opt/lce/reporter/ssl/`, the server-side SSL credentials for securing interaction with Log Correlation Engine Web UI are stored in the separate `/opt/lce/credentials/web_UI/` location.

Bug Fixes

- The `lced` daemon would discard its previous reading of activeDb size on failure to acquire a new reading; this could lead to inaccuracies in activeDb trim action scheduling.
- In certain cases `showids` would enter dynamic halt state while saving an alert, and fail to relinquish its PostgreSQL connection.
- The `lce_queryd` daemon would retrieve total event count from the `*_hhourly` rollup tables even given a too-narrow query timespan; as result, total event count shown in upper right-hand corner of Tenable Security Center's Event Analysis summary pages could be inaccurate for queries covered much less than 1 week, at sites with relatively low inflow volume.
- Because of the extremely conservative default value `False` of the `data_sync_retry` setting in its configuration, PostgreSQL can mistakenly infer disk record corruption from a single spurious I/O fault report from the OS. This behavior is not a PostgreSQL bug nor an LCE bug, but each manifestation occasions significant (30 to 60 minutes) unscheduled downtime. To prevent this issue, LCE installer will now set `data_sync_retry` to `True`.
- When the source IP of packets received from an Log Correlation Engine client changes (as can happen with DHCP and several other scenarios) from *A* to *B*, LCE should update said client's IP to *B* in its internal roster; instead, Log Correlation Engine would record a new client with IP *B*, and retain the record of same client at *A*. Overall result was apparently duplicate client roster entries.
- Certificate authentication of WebUI logins worked in some particular cases, but did not work in the general case.

- Some values of the `web_UI__password__minimum_lifetime__hours` configuration attribute could interfere with a newly created user changing password from the temporary SA-assigned password to normal.
- The `lce_wwwd` daemon could reserve up to 7 PostgreSQL DB connections, contributing to an out-of-connections error condition in certain rare circumstances; fixed so that `lce_wwwd` uses no more than 2 PostgreSQL DB connections.
- Policy editor failed to honor the setting to not monitor subdirectories, if selected.

Security Enhancements

- Prevent Cross Site Request Forgery (CSRF) on login screen by authenticating anti-CSRF tokens.
- Upgraded OpenSSL libraries to 1.1.1k .
- Removed support for the deprecated TLSv1.1 protocol variant.

Upgrade Notes

- If you are upgrading from a version earlier than Log Correlation Engine 4.8.4, upgrade to Log Correlation Engine 4.8.4 before upgrading to Log Correlation Engine 6.09.
- If you are upgrading from Log Correlation Engine 5.0.x, upgrade to Log Correlation Engine 5.1.1 before upgrading to Log Correlation Engine 6.0.9.
- If you are upgrading from Log Correlation Engine 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *Tenable Log Correlation Engine User Guide*.
- If you are upgrading from 6.0.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.5 or Later in the *Tenable Log Correlation Engine User Guide*.
- If you are upgrading from Log Correlation Engine 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.9-el6.x86_64.rpm
  ```

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, or 6.0.5, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr606-rebuild-hhourlies &
  ```

  > **Note:** The `upgr606-rebuild-hhourlies` script takes approximately 2.5 minutes to run per activeDb silo.

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr603-rebuild-silos &
  ```

  This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

  > **Note:** If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, run `/opt/lce/tmp/upgr606-rebuild-hhourlies` first, then `upgr603-rebuild-silos`.

- If you are upgrading from Log Correlation Engine 4.8.4, 5.1.1, 6.0, 6.0.1, 6.0.2, or 6.0.3, you may be prompted to run `/opt/lce/tmp/restore_per-client_decisions.sql` when the upgrade utility completes. If you receive this prompt and you performed explicit client authorizations (without the aid of client assignment rules or the auto-authorization setting) or specified custom sensor names for individual Log Correlation Engine clients, run:

  ```
  source /opt/lce/tools/source-for-psql-shortcuts.sh
  psqlf /opt/lce/tmp/restore_per-client_decisions.sql
  ```

  This script applies the changes you made to your upgraded Log Correlation Engine.

  > **Note:** If you did not perform explicit client authorizations or specify custom sensor names for individual Log Correlation Engine clients, you do not need to run `/opt/lce/tmp/restore_per-client_decisions.sql`

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Tenable Log Correlation Engine 6.0.8 Release Notes (01-21-2021)

> **Note:** Because CentOS 6 has reached end of life, Log Correlation Engine 6.0.8 is the last Log Correlation Engine release that will support CentOS 6. Tenable recommends upgrading to CentOS 7.

New Features

- The `archival-manager` utility, when invoked with `--list-snapshots`, now also displays the range of contained events' tOrigin as a pair of human-readable tstamps. For example: `2019Dec30 13:48:25 - 2020Jan01 05:00:53`.
- The `archival-manager` utility now lets you operate on multiple activeDb silos or archiveDb snapshots at once with the new command verbs *{* `--archive--range`, `--restore--range`, `--remove-active--range`, `--remove-archived--range`*}*. The commands take a <from_date> and a <to_date> argument, both in *YYYYMmmDD* format. For example: `2019Dec30`.
- New configuration attribute `internal_network_definedBy__include_networks` (boolean, defaults to `false`). If set to `true`, then when receiving a `showids` command containing a directional clause (`-dirinb`, `-dirout`, `-dirint`), Log Correlation Engine will take the IP ranges given by `include_networks` attribute as defining the internal network for the purpose of that `showids` command. Of this attribute and `internal_network_definedBy__mipfile1`, one must be `true` and one must be `false`.
- New `check_fix-file_accessibility` utility detects and fixes file accessibility problems like wrong ownership, wrong permissions, and inadvertently set immutable (`“i”`) extended file attribute.
- New `rebuild-rawlog-index.sql` helper script rebuilds index on the `rawlog` column. Required to apply modified TS (text search) configuration retroactively to events already stored.
- The `lced` daemon now saves `trimming_activeDb` and `trimming_archiveDb` alerts to give easier visibility into disk space management done by `lced`.

Changed Functionality and Performance Enhancements

- The `diag` utility now also detects and reports the following problems with client policy (`.lcp`) files:
  - Non-ASCII characters
  - Invalid characters in a `whitelist-hashes` or `custom-malware-hashes` element string
  - Illegal length of a `whitelist-hashes` or `custom-malware-hashes` element string
- The `throughput--kilo-eps.sql` helper SQL script now displays data with a variety of background colors, “heatmap”-style, to give you even clearer and faster insight into your Log Correlation Engine traffic volume over days and hour-to-hour.
- You can now bring up the `/opt/lce/tools/pg-helper-sql/` path without pressing Tab. You can press Enter to expand `psqlf SPACE w TAB` to `psqlf wal-activity.sql`. Now, `psqlf SPACE w TAB` , expands to `psqlf wal-activity.sql`, then press Enter.
- You no longer need to bring up the `/opt/lce/tools/pg-helper-sql/` path when invoking a helper SQL script with `psqlf`. Now, you can type `psqlf`, then press Space, then the first few letters of desired filename (e.g., `w a` if you want `wal-activity.sql`). Press Tab to complete, then Enter to run.
- Added `firewall_cisco_ftd.prm` with rules to normalize logs from Cisco Firepower Threat Defense (FTD) devices.
- Log Correlation Engine now specifies a log rotation policy for the `postgresql/server.log` tracelog so that the active tracelog file will not exceed 50 MB on average.

Bug Fixes

- Dynamic halt condition encountered in the 3rd inter-page transition of Quick Setup wizard; command-line workaround possible but not desirable.
- Fixed an issue where the `throughput--kilo-eps.sql` helper SQL script would display malformatted and incomplete output when invoked for a date range containing a daylight savings switchover date.
- Fixed an issue where the utilities `create--make-current--silo`, `reattach-partition`, and `query-plan-explainer` were not specifying non-default resource needs for their PostgreSQL sessions; as result, they ran slower than possible.

- When given a `-sumdate` command with `--sorttime --sort-descending` sort specifier, the `lce_queryd` daemon would under some circumstances preface its response with an incorrect header, ultimately leading to a skewed display in Tenable Security Center's Event Analysis Date Summary view.
- Fixed an issue where instead of showing the username of a newly created administrator-level user, the web UI would show "0".
- Fixed an issue where the `lce_queryd` daemon would fail to execute several summary queries when a particular combination of filters was specified.
- Fixed an issue where the `optimize-datastore` utility could interfere with the process of temporarily restoring an "archive peek" silo into activeDb.
- Fixed an issue where the `lce_wwwd` daemon could reserve up to 7 PostgreSQL DB connections, contributing to an out-of-connections error condition in certain rare circumstances; `lce_wwwd` now uses no more than 2 PostgreSQL DB connections.

Security Enhancements

- Upgraded `lodash` from 4.17.11 to 4.17.20.
- Upgraded `concat-stream` and `crypto-browserify`.
- Upgraded `shelljs` from 0.1.4 to 0.7.8.
- Updated `browser-pack` to 6.1.0.
- Upgraded `uglify-js` to 2.6.0.

Upgrade Notes

- If you are upgrading from a version earlier than Log Correlation Engine 4.8.4, upgrade to Log Correlation Engine 4.8.4 before upgrading to Log Correlation Engine 6.0.8.
- If you are upgrading from Log Correlation Engine 5.0.x, upgrade to Log Correlation Engine 5.1.1 before upgrading to Log Correlation Engine 6.0.8.
- If you are upgrading from Log Correlation Engine 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *Tenable Log Correlation Engine User Guide*.

- If you are upgrading from 6.0.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.5 or Later in the *Tenable Log Correlation Engine User Guide*.
- If you are upgrading from Log Correlation Engine 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.8-el6.x86_64.rpm
  ```

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, or 6.0.5, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr606-rebuild-hhourlies &
  ```

  > **Note:** The `upgr606-rebuild-hhourlies` script takes approximately 2.5 minutes to run per activeDb silo.

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr603-rebuild-silos &
  ```

  This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

  > **Note:** If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, run `/opt/lce/tmp/upgr606-rebuild-hhourlies` first, then `upgr603-rebuild-silos`.

- If you are upgrading from Log Correlation Engine 4.8.4, 5.1.1, 6.0, 6.0.1, 6.0.2, or 6.0.3, you may be prompted to run `/opt/lce/tmp/restore_per-client_decisions.sql` when the upgrade utility completes. If you receive this prompt and you performed explicit client authorizations (without the aid of client assignment rules or the auto-authorization setting) or specified custom sensor names for individual Log Correlation Engine clients, run:

  ```
  source /opt/lce/tools/source-for-psql-shortcuts.sh
  psqlf /opt/lce/tmp/restore_per-client_decisions.sql
  ```

This script applies the changes you made to your upgraded Log Correlation Engine.

> **Note:** If you did not perform explicit client authorizations or specify custom sensor names for individual Log Correlation Engine clients, you do not need to run `/opt/lce/tmp/restore_per-client_decisions.sql`

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Tenable Log Correlation Engine 6.0.7 Release Notes (01-19-2021)

> **Note:** Because CentOS 6 has reached end of life, Log Correlation Engine 6.0.7 is the last Log Correlation Engine release that will support CentOS 6. Tenable recommends upgrading to CentOS 7.

New Features

- The `archival-manager` utility, when invoked with `--list-snapshots`, now also displays the range of contained events' tOrigin as a pair of human-readable tstamps. For example: `2019Dec30 13:48:25 - 2020Jan01 05:00:53`.
- The `archival-manager` utility now lets you operate on multiple activeDb silos or archiveDb snapshots at once with the new command verbs *{* `--archive--range`, `--restore--range`, `--remove-active--range`, `--remove-archived--range`*}*. The commands take a <from_date> and a <to_date> argument, both in *YYYYMmmDD* format. For example: `2019Dec30`.
- New configuration attribute `internal_network_definedBy__include_networks` (boolean, defaults to `false`). If set to `true`, then when receiving a `showids` command containing a directional clause (`-dirinb`, `-dirout`, `-dirint`), Log Correlation Engine will take the IP ranges given by `include_networks` attribute as defining the internal network for the purpose of that `showids` command. Of this attribute and `internal_network_definedBy__mipfile1`, one must be `true` and one must be `false`.
- New `check_fix-file_accessibility` utility detects and fixes file accessibility problems like wrong ownership, wrong permissions, and inadvertently set immutable (“`i`”) extended file attribute.

- New `rebuild-rawlog-index.sql` helper script rebuilds index on the `rawlog` column. Required to apply modified TS (text search) configuration retroactively to events already stored.
- The `lced` daemon now saves `trimming_activeDb` and `trimming_archiveDb` alerts to give easier visibility into disk space management done by `lced`.

Changed Functionality and Performance Enhancements

- The `diag` utility now also detects and reports the following problems with client policy (`.lcp`) files:
  - Non-ASCII characters
  - Invalid characters in a `whitelist-hashes` or `custom-malware-hashes` element string
  - Illegal length of a `whitelist-hashes` or `custom-malware-hashes` element string
- The `throughput--kilo-eps.sql` helper SQL script now displays data with a variety of background colors, “heatmap”-style, to give you even clearer and faster insight into your Log Correlation Engine traffic volume over days and hour-to-hour.
- You can now bring up the `/opt/lce/tools/pg-helper-sql/` path without pressing Tab. You can press Enter to expand `psqlf SPACE w TAB` to `psqlf wal-activity.sql`. Now, `psqlf SPACE w TAB` , expands to `psqlf wal-activity.sql`, then press Enter.
- Added `firewall_cisco_ftd.prm` with rules to normalize logs from Cisco Firepower Threat Defense (FTD) devices.
- Log Correlation Engine now specifies a log rotation policy for the `postgresql/server.log` tracelog so that the active tracelog file will not exceed 50 MB on average.

Bug Fixes

- Fixed an issue where the `throughput--kilo-eps.sql` helper SQL script would display malformatted and incomplete output when invoked for a date range containing a daylight savings switchover date.
- Fixed an issue where the utilities `create--make-current--silo`, `reattach-partition`, and `query-plan-explainer` were not specifying non-default resource needs for their

PostgreSQL sessions; as result, they ran slower than possible.

- When given a `-sumdate` command with `--sorttime --sort-descending` sort specifier, the `lce_queryd` daemon would under some circumstances preface its response with an incorrect header, ultimately leading to a skewed display in Tenable Security Center's Event Analysis Date Summary view.
- Fixed an issue where instead of showing the username of a newly created administrator-level user, the web UI would show “0”.
- Fixed an issue where the `lce_queryd` daemon would fail to execute several summary queries when a particular combination of filters was specified.
- Fixed an issue where the `optimize-datastore` utility could interfere with the process of temporarily restoring an “archive peek” silo into activeDb.
- Fixed an issue where the `lce_wwwd` daemon could reserve up to 7 PostgreSQL DB connections, contributing to an out-of-connections error condition in certain rare circumstances; `lce_wwwd` now uses no more than 2 PostgreSQL DB connections.

Security Enhancements

- Upgraded `lodash` from 4.17.11 to 4.17.20.
- Upgraded `concat-stream` and `crypto-browserify`.
- Upgraded `shelljs` from 0.1.4 to 0.7.8.
- Updated `browser-pack` to 6.1.0.
- Upgraded `uglify-js` to 2.6.0.

Upgrade Notes

- If you are upgrading from a version earlier than Log Correlation Engine 4.8.4, upgrade to Log Correlation Engine 4.8.4 before upgrading to Log Correlation Engine 6.0.7.
- If you are upgrading from Log Correlation Engine 5.0.x, upgrade to Log Correlation Engine 5.1.1 before upgrading to Log Correlation Engine 6.0.7.

- If you are upgrading from Log Correlation Engine 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *Tenable Log Correlation Engine User Guide*.
- If you are upgrading from 6.0.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.5 or Later in the *Tenable Log Correlation Engine User Guide*.
- If you are upgrading from Log Correlation Engine 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.7-el6.x86_64.rpm
  ```

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, 6.0.2, 6.0.3, 6.0.4, or 6.0.5, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr606-rebuild-hhourlies &
  ```

  Note: The `upgr606-rebuild-hhourlies` script takes approximately 2.5 minutes to run per activeDb silo.

- If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr603-rebuild-silos &
  ```

  This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

  Note: If you are upgrading from Log Correlation Engine 6.0, 6.0.1, or 6.0.2, run `/opt/lce/tmp/upgr606-rebuild-hhourlies` first, then `upgr603-rebuild-silos`.

- If you are upgrading from Log Correlation Engine 4.8.4, 5.1.1, 6.0, 6.0.1, 6.0.2, or 6.0.3, you may be prompted to run `/opt/lce/tmp/restore_per-client_decisions.sql` when the upgrade utility completes. If you receive this prompt and you performed explicit client authorizations (without the aid of client assignment rules or the auto-authorization setting) or specified custom sensor names for individual Log Correlation Engine clients, run:

```
source /opt/lce/tools/source-for-psql-shortcuts.sh
psqlf /opt/lce/tmp/restore_per-client_decisions.sql
```

This script applies the changes you made to your upgraded Log Correlation Engine.

> **Note:** If you did not perform explicit client authorizations or specify custom sensor names for individual Log Correlation Engine clients, you do not need to run `/opt/lce/tmp/restore_per-client_decisions.sql`

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

2020 LCE

Log Correlation Engine 6.0.6 Release Notes (09-29-2020)

New Features

- The "archive peek" feature, present in LCE 4.x but either missing or inoperable in LCE 5.x, is again fully operational.
- Configuration attributes have been added to make optional and configurable the population of the 5 largest rollup tables, as well as indexing of several columns of the silo-partitioned `events` table; these attributes should be not be manipulated directly with `cfg-utils --set-sv`, but only with the new `toggle-augmented-event-lookups` utility. Please contact Tenable Support for help deciding which rollups you can disable without impacting your

accustomed queries.

- To allow desired operation in environments where LCE server is known by a public virtual IP even to non-NAT clients, added `public_IP_for_clients_not_behind_NAT` configuration attribute.

Changed Functionality and Performance Enhancements

- The `optimize-datastore` utility now also collapses rows in the rollup tables used to satisfy summary queries; this both decreases disk usage and improves query performance.
- 48-hour summary queries can now also take advantage of the rollup tables.
- Several new rollup tables have been added, for a total of 8; summary queries filtering on event type plus another attribute can now be satisfied with rollup tables, greatly improving performance of over 55% of built-in queries, as well as many custom queries.
- Text search configuration has been refined; as a result, indexes on rawlog column (of siloN tables created after upgrading to LCE 6.0.6) will be 5% to 20% smaller.
- More than just print snapshot names, `archival-manager --list-snapshots` now also reports, for each snapshot in archiveDb:
  - compressed on-disk size
  - compression level used (4 normally, 7 if `archiveDb__compress_tighter` enabled)
  - when snapshot had been written to archiveDb
  - whether you can "peek" query this snapshot (yes if snapshot had been created with LCE 6.0.6+, otherwise no)
- Progress is reported with higher granularity by `archival-manager --roll-currsilo-now`; it separately reports [a] when specified silo is no longer the current silo (i.e. new events are no longer being written to it); and [b] when the specified silo's post-roll housekeeping tasks are complete (i.e. utilities which need to temporarily detach silo they are operating on would no longer block on this one).
- To quickly learn ID of the silo new events are being written to, you can now `archival-manager --identify-currsilo`.

- The counters printed to tracelog by the `lce_queryd` daemon now report failure modes broken down into 5 categories, up from 3; this extends the amount of troubleshooting possible without debug having been configured.
- The helper scripts `alerts-by-day.sql`, `alerts-by-month.sql`, `table-sizes--silo.sql`, and `silos.sql` have been modified to report the same data but more compactly.
- The helper scripts `disk-usage.sql`, `indexes--other.sql`, `table-access-stats--other.sql`, and `table-sizes--nonsilo.sql` now take an optional table name fragment argument, to restrict output to only the matching tables.
- To improve output readability, many of the helper scripts which produce reports now render the background of every other row in an alternative dark color.
- Added the `reached_license_limit` alert occasion, so both operators and Tenable Support staff can more easily tell that LCE Server has been trimming activeDb to stay under license limit; along with other alerts, `reached_license_limit` will be in output of `alerts-by-day.sql`, `alerts-by-month.sql`, and `recent-alerts-24hours.sql` helper scripts.
- Before overwriting the local activeDb as part of full-DB `--restore-from` a given backup, the `online-pg-backup` utility now saves the license activation key (along with other node-specific configuration and status values) to a directory outside of activeDb; after the full-DB restore is complete, `online-pg-backup` retrieves those special values and updates the local activeDb with them. This makes moving an LCE instance from one host to another a significantly smoother process.
- The following utilities now trace, to facilitate troubleshooting, to `backup-and-restore.log`:
  - `online-pg-backup`
  - `port-controlfiles`
- The following utilities all now trace to `activeDb-maint.log`, instead of sharing `postgresql-setup-accretive.log` with installer/upgrader utilities as previously:
  - `archival-manager`, when invoked with `--roll-currsilo-now`
  - `create--make-current--silo`
  - `reattach-partition`

Bug Fixes

- To `firewall_checkpoint.prm`, added missing and requested `Checkpoint-TCP_Spoof` rule.
- Migration of a LCE 5.x silo into activeDb could fail if size of activeDb had reached maximum, whether due to availability of unused disk blocks or due to the configured `activeDb_max_on_disk_size__MB` having been reached.
- Invalid SQL generated for `-assetfile` summary query.
- Licensed limit of activeDb silos was checked only on startup of the `lced` daemon; hence applying a new license would require a restart of the `lced` daemon, entailing up to 55 seconds of lost incoming events.
- Optimization for queries involving single-address IP filters had been rendered dysfunctional.
- The `lce_report_proxyd` daemon would save a `vuln_report_upload_error` alert upon receiving credentials with an empty username from Tenable Security Center; since that happens when vuln upload has simply not been configured by customer, it does not constitute an error mode per se.
- Setting vuln reporter username/password from Web UI would cause unscheduled termination of the `lce_wwwd` daemon process.
- The `stats` daemon would, in certain unusual circumstances, skip over some events records instead of properly scanning them.
- The `install-logrotate-config` utility, when invoked by the RPM upgrader, would create a backup of the old LCE-specific logrotate configuration and save that backup in `/etc/logrotate.d` directory, potentially causing system administration problems. Fix both corrects said behavior and erases any logrotate configuration backups we had previously created in `/etc/logrotate.d` directory.
- SQL generated to satisfy a `showids` query with a `-dirinb|-dirout|-dirint` keyword was valid but functionally incorrect.
- The IP ranges comprising (for purposes of a `showids` query with a `-dirinb|-dirout|-dirint` keyword) the internal network were being computed in a manner inconsistent with description in User Guide; corrected, and added boolean configuration attribute `internal_network_definedBy__mipfile1` to allow reversion to old behavior if needed.

- The `port-controlfiles` utility did not correctly import client policies (`.lcp` files), when invoked with `--import` option.
- Could not add elements to the multi-valued `intrusion_detect_sensors` configuration attribute from the WebUI, for 3 particular IDS sources.
- The `lce_queryd` daemon would, under certain combinations of operational circumstances, fail to properly erase `mipfile.*` tempfiles created by Tenable Security Center in the `/tmp` directory.
- The `lce_queryd` daemon was not rejecting invalid `showids` commands with empty "`match=`" expressions.
- Total count for certain distinct-IP and distinct-port queries was reported as half its true value.
- The `lce_tasld` daemon was ignoring values of `include_networks` and `exclude_networks` configuration attributes.
- The `migrateDB-from4X` executable, invoked by `migrateDB-overseer` utility, was ignoring value (if non-default) of `activeDb_directory` configuration attribute.
- The `indexes--nonsilo.sql` helper script was not reporting correctly the `fillfactor` PostgreSQL storage parameter of subject indexes.

Security Enhancements

- Updated to the latest stable version of JavaScript libraries (`crypto-browserify`, `i18n`, `js-yaml`, `tilt`, and others) used in Web UI, in order to incorporate available security fixes.

Upgrade Notes

- If you are upgrading from a version earlier than LCE 4.8.4, upgrade to LCE 4.8.4 before upgrading to LCE 6.0.6.
- If you are upgrading from LCE 5.0.x, upgrade to LCE 5.1.1 before upgrading to LCE 6.0.6.
- If you are upgrading from LCE 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *LCE User Guide*.

- If you are upgrading from 6.0.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.5 or Later in the *LCE User Guide*.
- If you are upgrading from LCE 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.6-el6.x86_64.rpm
  ```

- If you are upgrading from LCE 6.0.x, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr606-rebuild-hhourlies &
  ```

  Note: The `upgr606-rebuild-hhourlies` script takes approximately 2.5 minutes to run per activeDb silo.

- If you are upgrading from LCE 6.0.x, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr603-rebuild-silos &
  ```

  This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

  Note: If you are upgrading from LCE 6.0, 6.0.1, or 6.0.2, run `/opt/lce/tmp/upgr606-rebuild-hhourlies` first, then `upgr603-rebuild-silos`.

- If you are prompted to run `/opt/lce/tmp/restore_per-client_decisions.sql` and you performed explicit client authorizations (without the aid of client assignment rules or the auto-authorization setting) or specified custom sensor names for individual LCE clients, run:

  ```
  source /opt/lce/tools/source-for-psql-shortcuts.sh
  psqlf /opt/lce/tmp/restore_per-client_decisions.sql
  ```

  This script applies the changes you made to your upgraded LCE.

> **Note:** If you did not perform explicit client authorizations or specify custom sensor names for individual LCE clients, you do not need to run `/opt/lce/tmp/restore_per-client_decisions.sql`

Log Correlation Engine 6.0.5 Release Notes (06-30-2020)

New Features

- Offline plugins updates can now be accomplished from command line: download and copy `lce-combined.tar.gz` to path you have designated with the new configuration attribute `offline_plugin_update__tarball_path`, then restart the `lce_www` service.
- To aid troubleshooting at HA (high availability) sites, `--track-packet-counts` option has been added to the `ha-manager` utility.
- Full list of all user accounts (both Web UI and nologin), helpful in some troubleshooting scenarios, is now available with `user-utils --list-all`.
- The output of `cfg-utils --describe <attributeName>` now includes the given attribute's install-time default value.
- New `show-config--mv--event_rules.sql` script, for much improved display of `event_rules` attribute from command line and in diag reports.
- New `useful-and-idle--plugins.sql` script, to report which PRM and TASL plugins are actively contributing, and how many events have been affected by each. Should you wish to disable in configuration the non-contributing ("idle") plugins, `useful-and-idle--plugins.sql` makes it easy: it prints an appropriate shell command, which you need only to copy-paste to console.
- New scripts have been added to help you need to pinpoint the day and hour when a particular source stopped sending data to LCE Server or compare event traffic volume across LCE Client sources. This suite of SQL scripts is divided into two groups:
  - To generate a temporary lookup table: `influx-trends--by--src-ip.sql` and `influx-trends--by--sensor.sql` (both parameterized by a date range); and `influx-trends--by--compound-profile--clients-only.sql` (parameterized by silo#).

    - To query a temporary lookup table: `_i_t_q__{hourly,daily,weekly,monthly}__{absolute,baseline_start,baseline_finish,coevals_rank,delta_immediately_previous}.sql`

- The date and time of the last successful login are now displayed in Web UI after login.

Changed Functionality and Performance Enhancements

- Maximum number of LCE Clients allowed to connect concurrently is now 20476, up from 8192.
- Average time to match a log against event rules has been roughly halved; customers with significant number of configured event rules may note increased throughput.
- The `reset-account` utility has been renamed to `user-utils` to reflect the broader functionality it now encompasses; it is located in the same `/opt/lce/tools` directory.
- The `cfg-utils` utility now performs even more input validation: for example, it will check an attempt to assign same port number to 2+ port number configuration attributes.
- The `optimize-datastore` utility now needs 5-8% less time to process a silo, in the default (i.e. neither `--also-cluster` nor `--also-reindex`) operating mode.

Bug Fixes

- After the `lce_client` service in Windows LCE Client installs restarted, in certain circumstances LCE Server would mistakenly create duplicate roster entries representing that client.
- Deleting a large number (over 200) clients through Web UI could cause the `lced` daemon to terminate abnormally.
- In certain circumstances which can arise particularly at high-volume sites, operation of the `optimize-datastore` utility could interfere with silo roll process, resulting in oversize silos and/or overall performance drop.
- An invalid event rule was accepted partially, instead of being rejected wholly, and such an incomplete rule would interrupt event normalization.
- Failure to run the PostgreSQL VACUUM command on `pm_clients__ephemera` table could impact response Web UI time with some unusual workloads.

- Output of `cfg-utils --get intrusion_detect_sensors` did not include the `customer_codes__comma_sep` attribute.
- Values in several columns of `status_client_counts` DB table, and Web UI pages populated therefrom, could diverge from expected.
- When the `lce_server` service is started from command line (whether directly or via `start-all` script or `restart-all` script), a few trace messages intended for `lced` tracelog are printed to console; this may give false impression that startup has not completed successfully.
- Adding a Web UI user from Web UI would add an account with username `0`, regardless of the username specified by operator.
- Web UI link for changing one's own password did not work consistently.
- Web UI controls for locking / unlocking a Web UI user did not function, for a particular subset of LCE Server installations.
- The minimum edit distance constraint, as configured by the `web_UI__password__minimum_edit_distance` attribute, was not enforced when changing one's own password in Web UI.
- The **Occasion** column in **Alerts** tab of Web UI was too narrow to accommodate some alert occasion names; in such cases, a single alert would take up extra vertical display space, reducing the overall number of alerts visible without scrolling.

Security Enhancements

Internal Audit Log for Actions Pertaining to Web UI User Accounts

- All account-admin actions (add acct, unlock acct, etc.) and session-scope actions (begin session, end session, etc.) with failure outcome are now tracked in this audit log.
- If so configured, LCE will also track session-scope actions (begin session, end session, etc.) with success outcome.
- If so configured, LCE will copy each audit entry to host syslog in real-time.
- If so configured, LCE will, furthermore, dumped this audit log to a backup location of your choice at an interval of your choice.

Enforce Your Site's Password Reuse Policy

- The password provided when adding a Web UI user account is now always considered a temporary password and the account owner must change it on first login.
- If configured, LCE will now enforce minimum and/or maximum password lifetime.
- If configured, LCE will now prevent a Web UI user from changing password to one used within the latest *n* password changes.
- If configured, LCE will now prevent a Web UI user from changing password to one differing by fewer than *n* characters (per Levenshtein edit distance) from the current password.

Enforce Your Site's Login Session Policy

- If configured, LCE will now automatically lock the account of a Web UI user who has attempted but failed to login at least *m* times within *n* consecutive minutes.
- If configured, LCE will now automatically lock the account of a Web UI user who has not been active within *n* consecutive hours.

Better Control of LCE Clients

- If configured, LCE will now automatically logout and revoke the authorization of a client which has been inactive within *n* contiguous days.

Upgrade Notes

- If you are upgrading from a version earlier than LCE 4.8.4, upgrade to LCE 4.8.4 before upgrading to LCE 6.0.5.
- If you are upgrading from LCE 5.0.x, upgrade to LCE 5.1.1 before upgrading to LCE 6.0.5.
- If you are upgrading from LCE 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *LCE User Guide*.
- If you are upgrading from 6.0.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.5 or Later in the *LCE User Guide*.
- If you are upgrading from LCE 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.5-el6.x86_64.rpm
  ```

- If you are upgrading from LCE 6.0.x to LCE 6.0.5, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr603-rebuild-silos &
  ```

  This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

- If you are prompted to run `/opt/lce/tmp/restore_per-client_decisions.sql` and you performed explicit client authorizations (without the aid of client assignment rules or the auto-authorization setting) or specified custom sensor names for individual LCE clients, run:

  ```
   /opt/lce/tmp/restore_per-client_decisions.sql
  ```

  This script applies the changes you made to your upgraded LCE.

  > **Note:** If you did not perform explicit client authorizations or specify custom sensor names for individual LCE clients, you do not need to run `/opt/lce/tmp/restore_per-client_decisions.sql`

AKZ NOTE: Upgrade notes from 6.0.4, in case edits are needed for 6.0.5

- If you are upgrading from a version earlier than LCE 4.8.4, upgrade to LCE 4.8.4 before upgrading to LCE 6.0.4.

- If you are upgrading from LCE 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *LCE User Guide*.

- If you are upgrading from LCE 5.0.x, upgrade to LCE 5.1.1 before upgrading to LCE 6.0.4.

- If you are upgrading from LCE 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.4-el6.x86_64.rpm
  ```

- If you are upgrading from LCE 6.0.x to LCE 6.0.4, after the `rpm` command completes, run:

```
nohup /opt/lce/tmp/upgr603-rebuild-silos &
```

This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Log Correlation Engine 6.0.4 Release Notes (05-11-2020)

New Features

- Direct-from-4X migration, using the same migrateDB-overseer interface used for direct-from-5X migration.
- HA support, configured with the new `utility ha-manager`.
- New utility `online-pg-backup`, for online backup (also known as hot backup) of LCE's PostgreSQL database.
- New utility `port-controlfiles`, to aid moving an LCE instance from one host to another.
- The alert *occasion code*, associated with alerts as of 6.0.3, is now displayed in Web UI where alerts are listed.
- An `activeDb_disk_device_I_O_saturated` alert will now be created when conditions warrant, to give you better visibility into resource thresholds.
- New option `--vlike` for the `cfg-utils` utility; it neither matches by nor shows old config attribute name, but does show (up to 50 characters of) the value of each matched config attribute.
- New helper script `alerts-by-month.sql`: `alerts-by-day.sql`'s longer-term counterpart.

Changed Functionality and Performance Enhancements

- Increased throughput, compared to previous versions, when the multi-valued configuration attribute syslog_sensors has many values.
- The `optimize-datastore` utility now resumes work more promptly, after a pause meant to prevent spikes in resource consumption; as consequence, `optimize-datastore` now needs less time per silo.
- With 30 seconds cut from the `lced` daemon's shutdown time, restarts are quicker and events loss window is smaller.

Bug Fixes

- When estimating disk size taken up by activeDb, the `lced` daemon would consider the entire activeDb directory, instead of just its postgresql/ subdirectory; at installations with pre-6X silos still present and stored in the activeDb directory, this would result in an over-estimate.
- The `lced` daemon would manifest a severe memory leak when configured to forward syslog over UDP.
- The `lced` daemon could fail to restart after having been abnormally terminated (e.g. due to sudden host power-off) while a silo roll was in progress.
- In the very rare case of PostgreSQL being restarted right after startup of the `lced` daemon, one of the `lced` daemon's `dbWriter` threads could fail to persist events.
- Generation of diag report could hang while recording sample of input to the LCE Netflow client, if that client is installed on same host.
- Diagnostics could be launched multiple times from the UI and link to report could be clicked before diag actually finished.
- When upgrading from pre-6.0.3 installations, values of the `event_rules` configuration attribute would not be correctly migrated.
- Prevent inadvertent concurrent execution of the `diag` utility.
- Network name of client hosts not populated.
- Timestamp of alerts as shown in WebUI would be displayed in UTC and not localtime.
- The `cfg-utils` utility would not accept values with embedded newlines.

- Upgrade from 6.0.0/6.0.1/6.0.2 would fail if the `postgresql` service had not been running at the time `rpm -U` was invoked.
- When upgrading from pre-6.0.3 installations, values of `syslog_forward_destinations__TCP` configuration attribute would not be correctly migrated.
- WebUI descriptions of several configuration attributes' required format were inaccurate and misleading.
- Only the first of multiple configured syslog sensors would be used by the `lced` daemon.
- The `optimize-datastore` utility could continue to run beyond the time limit given it by `--max-runtime-hours` flag.
- Conversion to UTF encoding of client-sent logs encoded in UTF16-LE failing in some cases.
- Current silo would not be queryable, if the `lced` daemon had previously been abruptly shutdown during a particular point in the silo roll sequence.
- Changes made in WebUI to the `HTTP_proxy__port` configuration attribute would not be persisted.
- Certain user-defined policies were unable to be deleted from the user interface.
- For several particular showids command types, the `lce_queryd` daemon would not fill in time-range upper bound if missing.
- Database index on silo tables' rawlog column not used unless configuration attribute `position_sensitive_text_search` set to true.
- Given a `showids` command with multiple positive filters on the same normalized dimension, such that some but not all of those filters specified dimension literals not in DB, the `lce_queryd` daemon would return 0 records.
- Restore of an archived silo snapshot could be incomplete, given mixed-case dimension literals.

Security Enhancements

- Added HTTP Content-Security-Policy header.
- Upgraded set of available cipher suites to prefer most secure and fall back on SHA-1 only for browsers that support nothing else.
- Upgraded Bootstrap to prevent cross-site scripting vulnerability.
- Upgraded jQuery and jQuery UI to prevent cross-site scripting and file upload vulnerabilities.
- Added HTTP Cache-Control header to prevent sensitive information from being cached by the user's web browsers.
- Upgraded Moment.js to prevent regular expression denial of service vulnerability.
- In publicly available URL, hide version numbers if not logged in.
- Pass session token only in server-side cookie, never in the URL.
- Added HTTP Strict-Transport-Security header.
- Added HTTP X-Content-Type-Options header.
- Added HTTP X-XSS-Protection header.
- Removed all client-side (JavaScript) cookie references.

Upgrade Notes

- If you are upgrading from a version earlier than LCE 4.8.4, upgrade to LCE 4.8.4 before upgrading to LCE 6.0.4.
- If you are upgrading from LCE 4.8.4 with high availability configured, use the method described in Migrate Your High Availability Configuration to LCE 6.0.4 or Later in the *LCE User Guide*.
- If you are upgrading from LCE 5.0.x, upgrade to LCE 5.1.1 before upgrading to LCE 6.0.4.
- If you are upgrading from LCE 5.x.y or 6.0.0, run:

  ```
  rpm --nopreun -Uvh lce-6.0.4-el6.x86_64.rpm
  ```

- If you are upgrading from LCE 6.0.x to LCE 6.0.4, after the `rpm` command completes, run:

```
nohup /opt/lce/tmp/upgr603-rebuild-silos &
```

This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Log Correlation Engine 6.0.3 Release Notes (02-04-2020)

New Features

- Query filter on log text may now specify that multiple tokens must be immediately adjacent in a particular order (examples follow). Token-adjacent search is disabled by default; enabling it costs a 10% to 15% increase in disk space needed for database indexes on event log text.
  - Example: `text='nodeA success'` will match both "nodeA success then nodeB failure" and "nodeA failure then nodeB success", just as in previous LCE releases. However, `text='"nodeA success"'` will match "nodeA success then nodeB failure" only; it will not match "nodeA failure then nodeB success."
  - Example: `text='NodeA Success'` is like `grep NodeA file.txt | grep Success`, whereas `text='"NodeA Success"'` is like `grep 'NodeA Success' file.txt`.
- The `v__events` view now has several additional columns, to permit fine-grained visibility into event normalization. These are:
  - `prm_id`: identifies the exact PRM rule which had normalized this event.
  - `prm_file`: filename (.prm) of the plugin containing the PRM rule which had normalized this event.
  - `tasl_file`: filename (.tasl or .nbin) of the TASL plugin which generated this event.

- The `v__events` view's `kind` column will now show `stats`, for events which had been generated by the `stats` daemon. This makes `stats` troubleshooting easier and faster.
- For every alert created, LCE Server now stores a corresponding *occasion* code: `cannot_DNS_resolve`, `client__too_long_inactive`, `license_expired`, `silo_archival_error`, etc. So you can now effectively summarize recent LCE activity, with help of these new scripts under `/opt/lce/tools/pg-helper-sql`:
    - `recent-alerts-24hours.sql`: show alert counts by occasion, grouped by hour for the past 24 hours; hours without alerts are omitted; alert occasions with zero occurrences are omitted. Great for on-the-spot checks.
    - `recent-alerts-14days-list.sql`: show alert counts by occasion, grouped by day for the past 14 days; days without alerts are shown; occasions with zero occurrences are shown. Excellent for comparing behavior of multiple LCE instances, or of the same LCE instance over successive weeks.
- Further about alert occasions: the new `disabled_alert_occasions` configuration attribute (not accessible from web UI for now) lets you specify occasions of alerts you do not want created; this lets you curtail "alert spam" proactively.
- New script `ts-stats.sql`, under `/opt/lce/tools/pg-helper-sql`, is intended to aid troubleshooting of text search (TS) functionality. It will help you figure out what custom stopwords to add, in order to decrease disk space needed for database indexes on event log text without impairing the queries you want.

Changed Functionality and Performance Enhancements

- As a result of switching to a more compact column representation, database silo tables will use 3% to 5% less disk space (versus LCE 6.0.0-6.0.2, for an equivalent number of events).
- With update of the embedded events datastore from PostgreSQL 11 to PostgreSQL 12, database indexes will use 20% to 40% less disk space (versus LCE 6.0.0-6.0.2, for an equivalent number of events).
- Write overhead has been decreased, and query performance has been improved, for many use scenarios.
- The `reset-login-account` utility has been renamed to reset-account; usage is unchanged.

- The `lce_cfg_utils` utility has been replaced with `cfg-utils`, offering far superior argument validation and error reporting; invoke with `--help` to see the legal usage.
- The `configure-pgServer-forPerformance` script now also takes into account how much swap space has been made available to the Linux OS; this lets us allocate RAM more conservatively at sites with low swap configurations, and thus avoid out-of-memory (OOM) aborts.

Bug Fixes

- The `lce_wwwd` daemon could crash, reporting segmentation fault, while shutting down.
- Shutdown of the `lced` daemon could hang, if TCP syslog forwarding and/or cloud vulnerability report upload were configured.
- Query results were not sorted in alphabetical order as per the `--sortevent`, `--sortsen`, `--sorttype`, or `--sortuser` query modifiers.
- In cases of high log influx volume, silo rolling would fail to complete promptly, resulting in oversize silos.
- Spurious `"events-vs-rollup discrepancy"` error messages appeared in `lced` daemon's tracelog.
- The `lced` daemon would, in certain exceptional circumstances, crash right after completing a silo roll.
- Some `+text='...'` query predicates were not translated to SQL predicates correctly.
- Could not edit already-created client assignment rules from web UI.
- Failed to persist changes to some settings configurable in *Config* > *Advanced* page of web UI.
- Evaluation of client assignment rules did not respect the special 0.0.0.0/0 pseudo-subnet.
- Policies with different filenames but exact same content (e.g. cloned or copied policies) were rejected.
- The `throughput--kilo-eps.sql` helper script would provide only partial results, if selected time range straddled a DST calendar boundary.

- Tenable Security Center's Detailed Event Summary tool would fail given some events normalized from Fortigate logs.
- In some rare cases, `optimize-datastore` utility would not re-attach silo partitions.
- In certain rare cases, the `lced` daemon would temporarily stop persisting new events.

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Upgrade Notes

- If you are upgrading from LCE 5.0.x, you must upgrade to LCE 5.1.1 before upgrading to LCE 6.0.3.
- If you are upgrading from LCE 6.0.0 or LCE 6.0.1 directly to LCE 6.0.3, before upgrading to 6.0.3, run:

  ```
  service postgresql start
  source /opt/lce/tools/exigent-sessions.bashrc
  pgConf=/opt/lce/db/postgresql/postgresql.conf
  grep -q '^[ \t]*temp_tablespaces\>' $pgConf && sed -i '/^[ \t]*'temp_
  tablespaces'\>/ d' $pgConf && su-psqlc "DROP TABLESPACE IF EXISTS sortspace"
  ```

  Tip: If you moved your database directory, replace `/opt/lce/db` with the correct path.

- If you are upgrading from LCE 6.0.x to LCE 6.0.3, after the `rpm` command completes, run:

  ```
  nohup /opt/lce/tmp/upgr603-rebuild-silos &
  ```

  This command rebuilds your pre-existing event silos in the new format (which takes up less disk space and improves query performance). As each silo is rebuilt, it will automatically become available for querying again. The `upgr603-rebuild-silos` script will take 25-30 minutes to rebuild each pre-existing silo; it prioritizes silos with the most recent events.

2019 LCE

Log Correlation Engine 6.0.2 Release Notes - 2019-10-17

> **Note:** Before upgrading 5.0.x to 6.0.x, upgrade and migrate to 5.1.1.

New Features

- New command-line utilities, all under `/opt/lce/tools/`:
  - `populate-missing-rollups`, to rectify the incomplete population of rollup tables for one or more `siloN` tables, should that ever occur. (Not intended or needed for normal operation.)
  - `reattach-partition`, to rectify partial attachment of a `siloN` partition table to the `events` pseudo-table, should that ever occur. (Not intended or needed for normal operation.)
  - `reset-login-account`, to reset the password for one of the secured accounts used to login to an LCE Server instance from outside the instance's host, if the LCE Web UI is for some reason unavailable or an operator simply prefers a console interaction for the purpose.

    > **Note:** Only the username is to be specified as a command-line argument. Once running, the utility will prompt you for a password.
- New options supported by existing command line utilities:
  - `optimize-datastore` now supports `--also-reindex`, `--also-cluster`, and `--max-runtime-hours` <M>. See the LCE 6.0.x User Guide for details.
- New helper scripts, all under `/opt/lce/tools/pg-helper-sql/`:

- `dimension-occurrence-stats.sql`, permits insight into distribution of the normalized dimensions (event1, event2, sensor, type, user) among stored events, see the LCE 6.0.x User Guide for details.
- `throughput--kilo-eps.sql` , shows volume of event influx, by the hour in units of 1000 events per second, see the LCE 6.0.x User Guide for details.

Changed Functionality and Performance Enhancements

- Re-implemented 4.x's chain-of-custody feature, which had been missing in 5.x releases.
- Optimization: queries filtering on single IP address now take advantage of indexes on the `src_ip` and/or `dst_ip` columns of events table, obviating use of the filter pointers mechanism which has a higher overhead.
- Optimization: histogram-type queries now can leverage consistent sampling, trading marginal accuracy for significant speedup.
- Optimization: `-assetsummary` queries now can leverage consistent sampling, trading marginal accuracy for significant speedup.
- All the helper `.sql` scripts prompt for arguments when invoked in interactive mode.
- Extended `diag` tool to generate more comprehensive reports, to facilitate faster troubleshooting.
- Re-implemented parts of logic in the `optimize-datastore` utility, to reduce interference with normal indexing and querying operations.
- FIPS-compliant mode.

Bug Fixes

- Corruption or loss of clients-policies map data was possible under certain circumstances.
- One or two apparent half-hour gaps were displayed in 24-hour histogram summaries.
- Expected content could be missing when drilling down on events in reports.
- Restoring an archived snapshot could be too slow.
- Had observed high latency and/or incorrect results with `-assetsummary` queries.

- Shutdown of the `lce_server` daemon was needlessly slow.
- Config module was wrongly rejecting the special value 0 of the `archive-size` config attribute.
- An internally generated event would not displayed correctly in a report context, if said event's log contained embedded newlines.
- Histogram query latency, in the case of very large datasets, was too high because not taking advantage of sampling.
- When rolling silos with archiving enabled, the oldest archived snapshots were not being trimmed to make space when needed.
- Queries lacking `-endtime` parameter were not eliciting correct response.
- In some cases, `import_logs` could fail to normalize events which `lced` would have normalized.
- Silo rolling could fail if silo numbers had been chosen out of sequence.
- The `lced` daemon could terminate abnormally if client logins occurred in a particular sequence.
- Event rules containing shell command not executing under some certain conditions.

Supported Platforms

- Red Hat Enterprise Linux 5 64-bit / CentOS 5 64-bit
- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Log Correlation Engine 6.0.1 Release Notes - 2019-06-25

> **Note:** Before upgrading 5.0.x to 6.0.x, upgrade and migrate to 5.1.1.

New Features

- New command-line utilities, all under `/opt/lce/tools/`:
  - `ts-test`, for checking how a particular log would be tokenized for the purpose of text search indexing, and whether a particular text search phrase would match it.
  - `validate-PRM-regex`, for checking whether a regex as specified in a custom `.prm` definition would match a particular log.
- New helper scripts, all under `/opt/lce/tools/pg-helper-sql/`:
  - `disk-usage-summary.sql`, gives a concise summary of disk usage by table category (tables which store events, tables which maintain filter pointers, rollup counts tables, etc.).
    - Output of this script has been added to `diag` report, to facilitate troubleshooting.
  - `drop-indexes-on-older-silos.sql`, allows operator to easily free up disk space by dropping indexes on silos which have not yet been archived/trimmed out of activeDb but are no longer queried. (Indexes can be easily regenerated later if needed.)
  - `coverage-by-hhour.sql`, displays a concise infographic of rollup counts coverage of the events in a given silo, with half-hourly granularity.
    - Output of this script has been added to `diag` report, to facilitate troubleshooting.
  - `presence-dim-by-hhour.sql`, displays a concise infographic of the presence of a particular type (or user, or sensor, or ...) among the events in a given silo, with half-hourly granularity. This can provide a bare-bones reporting capacity even when Tenable Security Center connection is interrupted.

Changed Functionality and Performance Enhancements

- Optimization: queries filtering on single IP address now take advantage of indexes on the `src_ip` and/or `dst_ip` columns of `events` table, obviating use of the filter pointers mechanism which has a higher overhead.
- Optimization: queries over extensive time ranges now can leverage consistent sampling, trading marginal accuracy for significant speedup.
- The `full-processes.sql` and `watch-processes.sql` scripts now correctly group PostgreSQL backend processes by client, then by work group.

- The `table-sizes.sql` script now breaks down each table's disk usage by free space map, transaction visibility map, in-line tuples, indexes on in-line tuples, out-of-line data, and indexes on out-of-line data.
- The `tasl.log` report of `.tasl` and `.nbin` script execution statistics is now first emitted 10 minutes after `lce_tasld` startup; and it can also be emitted on command at any time thereafter, upon receipt of `SIGRTMIN+10` signal.
- The `X_hhourly` tables are now `LOGGED`, and hence will not lose data in the event of abnormal termination of the main PostgreSQL process.
- The `source-for-psql-shortcuts.sh` script now automatically sets the `PGTZ` environment variable; this ensures that timestamps, in the results of queries invoked via `/opt/lce/postgresql/bin/psql`, are shown in the correct timezone.

Bug Fixes

- Windows OS version of LCE client hosts was being shown as Windows 2008 in Web UI, regardless of actual Windows OS version.
- Data Migration from LCE 5 could fail, under a narrow set of circumstances.
- Type (or user, or sensor, or ...) literals were not being properly substituted in the responses to `showids` queries, in some cases.
- Scanning of new events by `lce_tasld` daemon did not keep pace with creation of new events by `lced` daemon.
- Scanning of new events by `lce_tasld` daemon could fail to progress to a subsequent silo.
- Scanning of new events by `stats` daemon could fail to progress to a subsequent silo.
- Text queries containing stopwords and/or SQL-reserved punctuation did not return expected results.
- The `optimize-datastore` utility would take too long to complete, because it did not skip already-processed tables.
- Parallel processes forked by the `optimize-datastore` utility could cause inordinate contention.
- Needlessly aggressive cancellation of executing SQL queries was being done during silo roll.

Supported Platforms

- Red Hat Enterprise Linux 5 64-bit / CentOS 5 64-bit
- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Log Correlation Engine 6.0.0 Release Notes - 2019-04-30

New Features and Changed Functionality

> **Note:** Users should anticipate needing up to 40% *more* disk space in LCE 6.0.0 than what was required in LCE 5.x.

- LCE now uses PostgreSQL as the backend datastore.
- Datastore schema now includes several additional columns useful for troubleshooting and performance tuning; and a new vw__events view for easy ad-hoc SQL queries.
- Having eliminated external dependencies makes for a vastly simplified installation process.
- Improved built-in I/O monitoring, by having the lced daemon periodically collect and trace device-level statistics for the block device which stores the activeDb.
- The PostgreSQL maintenance commands requisite for optimal query performance have been collected into the /opt/lce/tools/optimize-datastore script. It is suggested that you run this script during off-peak (low-load) hours, preferably every day, perhaps triggered by a cron(1) job. The contained commands are very resource-intensive, so query performance could be degraded during the time that optimize-datastore is being run.
- Performance of certain drilldown queries can be improved by running the /opt/lce/tools/cache-filter-pointers utility at operator's discretion.
- By default, to enhance LCE performance, Tenable Security Center repository-defining address ranges no longer filter Events Analysis query results in some limited circumstances. If you require the repository-defining address ranges to filter query results in all cases, please contact Technical Support for guidance on changing this default.

Bug Fixes

- Sensor Summary query can return an empty string in the Sensor column.
- Ignoring some legal values of the `ssl-tls1p2-only` configuration attribute.
- No events generated by `stats` daemon.
- An extra UTF8 BOM (byte-order mark) is prepended when forwarding syslog.
- Windows and Linux LCE clients show *Disconnected* status intermittently.
- Insecure transmission of WebUI credentials in the context of file upload.

Supported Platforms

- Red Hat Enterprise Linux 5 64-bit / CentOS 5 64-bit
- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit
- Red Hat Enterprise Linux 7 64-bit / CentOS 7 64-bit

Upgrade Notes

> **Note:** Before upgrading 5.0.x to 6.0.x, upgrade and migrate to 5.1.1.

> **Note:** Tenable Security Center Dashboards and Reports will not display results for data in LCE 5.x event silos, until those LCE 5.x silos have been migrated to the LCE 6.x format.

- Users should anticipate temporarily needing up to 120 GB *more* disk space while migrating LCE 5.x silos to LCE 6.x format.
- If your upgrade path skips versions of LCE (e.g., upgrading from 5.0.0 to 5.1.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.
- Prior to beginning an event silo migration from LCE 5.x to LCE 6.0.0, users should ensure that there will be sufficient disk space, since a silo in the LCE 6.0.0 datastore (PostgreSQL) format will require more disk space than the same silo in the LCE 5.x datastore (Elasticsearch)

format. Users should anticipate needing up to 40% more disk space for a silo migrated to LCE 6.0.0 from LCE 5.x.

- To upgrade event silos from LCE 5.x format, execute, after running the RPM upgrade:

  ```
  /opt/lce/tools/migrateDB-overseer --migrate-all [--clear-source-on-success]
  ```

LCE Windows Client 5.0.2 Release Notes - 2019-03-19

Bug Fixes

- Fixed an issue that resulted in the LCE Windows Client version being displayed incorrectly in the LCE Server admin UI.
  - Due to a caching feature on the LCE server, LCE Windows Clients that were previously connected to LCE Server before upgrading to LCE Windows Client 5.0.2 will initially continue to display their previous version number in the LCE Server admin UI. To refresh the display after upgrading to LCE Windows Client 5.0.2, simply revoke and re-authorize the client.
- Fixed multiple issues related to the LCE Windows Client intermittently disconnecting from the LCE server.
- Fixed an issue that could cause the LCE Windows Client to become unauthorized from the LCE server.

Diagnostic Improvements

- More accurate and extensive client-side trace logging is now available, to facilitate troubleshooting when needed.
- New batch file now included in the LCE Windows Client for collecting diagnostic information.

Supported Platforms

- Windows Server 2008/2012/2012 R2/2016 and Windows 7/8/10

LCE OPSEC Client 4.5.0 Release Notes - 12/11/2018

Changed Functionality and Performance Enhancements

- Updated to use the SHA-256 Cryptographic Hash Algorithm, allowing interoperability with Check Point R80+ Management Center.
- LCE Server and LCE OPSEC Client may now be installed on the same host system.
- Statically linked against standard libraries to simplify installation dependencies.

Bug Fixes

- Fixed a bug that caused ingested logs containing quotation marks and/or newline characters to be split and unnormalized by LCE.

Supported Platforms

- Red Hat Enterprise Linux 6 64-bit / CentOS 6 64-bit

2018 Tenable Log Correlation Engine

Log Correlation Engine 4.8.4 Release Notes - 8/14/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Improvements

- Startup latency of the lced daemon has been reduced by over 60 seconds; this means less downtime in the event of LCE services restart.
- As a result of changed gzip compression parameters, DB file compression will now be significantly (20% to 70%) faster, while compressed DB files will use 1 to 4% more space.

  > **Note:** Observable speedup of discrete operations may vary.

- The stats daemon now saves an alert on startup. If the current LCE configuration precludes it from producing stats-type events.
- The install-logrotate-config utility, in /opt/lce/tools/. It generates a specialized config stanza, leveraging logrotate(8) to manage disk space needed for LCE tracelogs.
- More reliable and detailed reporting of any errors occurring during file compression and decompression.
- Fine-grained (by client IP and/or by event name) debug tracing now available, for more effective troubleshooting if needed.

Resolved Items

- The lce_tasld daemon becomes unstable and fails to produce TASL events, if a particular volume and pattern of input events are encountered.
- Memory leaks, and subsequent unscheduled restart, of the lce_tasld daemon.
- After invocation of certain config scripts, the current month's tracelog of the lced daemon can become non-writeable by lced itself.

File Names & MD5 Checksums

File	MD5
lce-4.8.4-el5.x86_64.rpm	809445e88198da535653e313273847bd
lce-4.8.4-el6.x86_64.rpm	fc6b1049bb3248dcd2df6a39f0617632
lce-4.8.4-el7.x86_64.rpm	d39758904ba25c344d8ada911a421b24

Log Correlation Engine 5.0.6 Release Notes - 6/26/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Improvements

- The diagnostics tool `diag` now records firewall configuration information, as well as additional directory information useful in diagnosing directory permissions problems.
- The `admin` utility, in `/opt/lce/tools/es-helper-scripts/`, now takes an additional option, `--filter-tracelog--errors-exceptions`. This filters the Elasticsearch tracelog and prints a succinct chronological listing of error messages and exceptions; in such a listing, redundant and non-actionable lines are excised.
- The `rectify-disk-utilization` utility, in `/opt/lce/tools/es-helper-scripts/`, is new. Intended for recovery from a full-disk situation, this utility helps an operator to bring disk usage to below 90%, in two phases:
  - erases non-critical files
  - as needed, repeatedly prompts operator to clear the oldest silo.
- The `harmonize-datastore` utility, in `/opt/lce/tools/es-helper-scripts/`, has been revised for greater robustness, as well as extended scope: it now corrects any errors in mapping of aliases to Elasticsearch indexes.

Resolved Items

- Authorized clients may lose authorization once disconnected.
- Authorization does not follow a client across an IP change.
- Daemon `lced` may terminate abnormally if size of the current silo far exceeds 20GB.
- Daemon `lce_tasld` becomes unstable and fails to produce TASL events, if a particular volume and pattern of input events are encountered.

- Daemon `lced` may terminate abnormally if a version 5 client fails to complete its login sequence.
- Excessive alerts generated when the `lced`daemon detects that a client's IP has changed.
- Installer improperly rejects certain versions of the OpenJDK JVM.
- Incorrect numbering of silos created by the `import_logs` utility.

File Names & MD5 Checksums

File	MD5
lce-5.0.6-el5.x86_64.rpm	3928e3e6f41f2b1beb67a64f28912ca5
lce-5.0.6-el6.x86_64.rpm	128b99c052101b9f86bd0bd3626bf27a
lce-5.0.6-el7.x86_64.rpm	8f8bac072500675bd6db69dd0624074c

Log Correlation Engine 5.1.0 Release Notes - 8/28/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New

The following are the new improvements included in LCE 5.1.0:

- Startup latency of the lced daemon has been reduced by over 60 seconds; this means less downtime in the event of LCE services restart.
- Response latency and completion time of LCE initscripts have been reduced, so service lce <serviceName> commands will now be more responsive.
- The stats daemon now saves an alert on startup, if the current LCE configuration precludes it from producing stats-type events.

- The diagnostics tool diag now also collects:
  - Additional host and networking configuration which could have bearing on LCE installation and operation.
  - (only if activeDb and/or archiveDb are in NFS-mounted partitions) NFS-specific configuration.
  - Indication of whether Linux kernel has had a FIPS mode enabled.
  - User-created and user-modified .prm plugins.
  - Creation times, in addition to modification times, of critical datastore and configuration files.
  - Roll-up summaries of connected clients, grouped by recent behavior and by assigned policy.
  - An extra list of client policy files, grouped by checksum and with any duplicate-content files clearly marked.
- The install-logrotate-config utility, in /opt/lce/tools/, is new. It generates a specialized config stanza, leveraging logrotate(8) to manage disk space needed for LCE tracelogs.
- The list-policies utility, in /opt/lce/tools/, is new. It lists on-disk policy files with basename parts color-coded for easier review, and also prints policy creation times.
- The save-customizations utility, in /opt/lce/tools/, is new; it is intended for situations where backup of LCE configuration, rather than events data, is desired.
- The harmonize-datastore utility, in /opt/lce/tools/es-helper-scripts/, has a new “dry-run” mode, enabling operator to preview steps to be taken.
- The list-clients utility, in /opt/lce/tools/, will now also report the agent software patchlevel. Also, this utility now accepts --flat option, to omit the header and then print all the columns per client on the same line; this is intended to ease post-processing.
- To help troubleshoot unnormalized logs, the lced daemon offers a special mode, which is activated by setting the save-nonmatched config attribute. This mode has been re-implemented to provide a more representative sample with less performance overhead; also, the meaning of save-nonmatched has changed: if it is N, lced will print, to its normal tracelog, approximately every Nth unnormalized log encountered.

Resolved Items

- Given certain syslog input combinations, TASL correlation engine crashes frequently.
- SQLite3 databases (lce_status.db, pm.db, lce_alerts.db), used to store operational state, can become effectively read-only under certain conditions, causing LCE daemons reliant on those databases to terminate abnormally.
- Non-default client policy assignments are not permanent.
- Under certain circumstances, Linux and Windows tail clients do not stay connected.
- Timestamp of logs in SecurityCenter reports, when such a report is exported in CSV format, is zeroed.
- Plugin update is skipped if the lce_wwwd daemon is restarted within 72 hours of initialization.
- Under certain conditions, Windows clients enter an infinite re-authorization loop.
- No more than 10,000 records returned by lce_queryd daemon even when -maxlimit query parameter specifies otherwise.
- Excess tracelog messages emitted, and alerts saved, when a client disconnects.
- Request to list archived snapshots periodically sent to Elasticsearch when archiving is not configured, resulting in spurious error messages.
- Invalid SQL generated and submitted by lce_wwwd daemon, in response to certain user administration operations.
- Clients not auto-authorized when auto-authorize-clients-time config attribute set.
- If a policy is assigned to one or more clients while LCE Server is shutdown, on startup of LCE Server those clients may become de-authorized.

File Names & MD5 Checksums

File	MD5
lce-5.1.0-el5.x86_64.rpm	37dfa06460879294a05c01fc17b4e20d
lce-5.1.0-el6.x86_64.rpm	dd1d3bbc4ca69d0f8a1b896d34d91d73
lce-5.1.0-el7.x86_64.rpm	ff0ac95a07acaa3f764ab21d46a35d29

Log Correlation Engine 5.1.1 Release Notes - 10/23/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

New Features

The following are the new features included in LCE 5.1.1:

- Extended error checking done by migrateDB-toES utility.
- The diagnostics tool diag now also:
  - Reports which, if any, particular rows in the pm.db SQLite3 database indicate a possible incongruity in client-dispatch operation.
  - Produces a concise overview of disk usage, in the new disk_usage_highlights.txt section.
- Upgraded OpenSSL to 1.0.2p.

Bug Fixes

- Certain WebUI pages unresponsive on login.
- Under certain conditions, events transmitted by Windows clients are not registered.
- Failure to strip newlines embedded in some logs sent by Windows clients, prior to persisting logs; if such a log is later retrieved to satisfy certain SecurityCenter queries, responses to those queries will consequently be malformatted.
- With a large number (above 4,000) of clients, client authorization can sporadically fail.

File Names & MD5 Checksums

File	MD5
lce-5.1.1-el5.x86_64.rpm	7628e2177f3b24d281bdef106e36ece3
lce-5.1.1-el6.x86_64.rpm	45236d61a4739fb1b4fac2dd48bd37e3
lce-5.1.1-el7.x86_64.rpm	bb869b2f416e312be3c0d59c37473cd2

Log Correlation Engine 5.0.3 Release Notes - 02/22/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 5.0.3, significant enhancements to LCE, and information about upgrading.

Improvements:

- Metadata support for document-lifecycle compliance use cases:
  - For every silo, now track the provenance of events therein; for new silo, this is “recordLive”, “migrateDst”, or “importLogs”.
  - Events of distinct provenance can enter the system concomitantly, but are never stored in the same silo as had been the case with LCE 5.0.0-5.0.2 (for legacy silos created with LCE 5.0.0-5.0.2, upgrader sets provenance “mixed”).
  - For customers with a regulatory or policy obligation to erase events older than N years, dedicated silos mean a vastly simplified erasure process.
- Elasticsearch performance and storage efficiency:
  - Instead of just handing Elasticsearch all the memory reserved for it without any detailed directions, we now issue directives explicitly allocating:
    - 13% to direct (i.e. not abstracted as objects within JVM heap) buffers, for decreased overhead of I/O operations in general.

        - 25% to JVM-hosted heap buffers dedicated to indexing operations, for higher and more stable indexing throughput.
        - 17% to JVM-hosted query cache, for better performance of frequent queries.
    - Optimized event data representation in the Lucene indexes underlying an Elasticsearch datastore, decreasing (by 19% with our testing data) the disk space required to store event data. Besides increasing storage ROI for our customers, this also improves query latency and indexing throughput.
- Clients/policies administration:
    - Decreased response time for `lce_client_manager`, the general CLI clients/policies administration utility.
    - Added `list-clients`, a dedicated lightweight CLI utility for the very common operation of querying status of connected clients, with minimal overhead.
- Datastore administration (for advanced users):
    - Added the multi-use CLI utility `es-helper-scripts/archival`, for a way to:
        - restore all silos within a specified date range, a much-requested feature.
        - view, for an archived snapshot, the provenance (see above) and count of events contained in that snapshot.
        - cancel a started, but incomplete, archive job.
    - Added the dedicated CLI utility `es-helper-scripts/move-activeDb`, for changing location of active DB from the default.
    - Added the dedicated CLI utility `es-helper-scripts/register-archiveDb`, for setting up location of archive DB.
- Site status data collection (for troubleshooting by Dev/CS/Pre-sales):
    - The largest files in directories commonly responsible for low-disk conditions.
    - Elasticsearch-internal: discrete operations, currently running tasks, queued tasks.
    - Operating parameters, garbage collection status of JVM running Elasticsearch.

Security Enhancements:

- Upgraded OpenSSL to 1.0.2n

Resolved Items:

- Fixed issue where an LCE instance becomes unregistered after restart
- Fixed unexpected results being returned for queries using Asset filters
- Fixed an issue that caused LCE clients to go offline
- Fixed several related issues causing lce_status.db, pm.db corruption
- Fixed an issue where ElasticSearch could not be started from GUI
- Fixed the Java version not being detected properly
- Performance and stability fixes to migration utility
- Fixed an issue where queries would remain open until a restart
- Fixed events messages being shown in the wrong columns of SC
- Fixed an issue where a single sensor could be tracked as 2+ sensors
- Fixed occasional corruption/elision of initial bytes in logs from Windows clients
- Fixed crash occurring if, with archiving on, `active-size` limit was reached
- Identified cause of zombie processes piling up at one particular customer site
- Fixed multiple installer issues

File Names & MD5 Checksums

File	SHA256	MD5	SHA1
lce-5.0.3-el5.x86_64.rpm	288727b2777716afcd9cb137149c50e930af0d242c7518345ed666fcec9561b5	820598d13c78c640ca4d0442e692a625	N/A
lce-5.0.3-el6.x8	c04a1fb67d03d51ce1b2144db6e7fe611964a9f1da445b81fb874b29438e6c4c	c048688f9f0f2f2eb9807877c6815433	N/A

File	SHA256	MD5	SHA1
6_64.rpm			
lce-5.0.3-el7.x86_64.rpm	d60266b840eaa2805b48ee532178d7f22fb1664090b1d9d64ce95333a723b0ac	f1d5a0075606684eab4257f2f75b1fdb	N/A

Log Correlation Engine 5.0.4 Release Notes - 4/24/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 5.0.4, significant enhancements to LCE, and information about upgrading.

Improvements:

- More detailed diagnostic messages traced when updating plugins from feed.
- Fine-grained trace selector mechanism now available, to facilitate troubleshooting of client login/dispatch. Selectors provided are:
  - `LCEfgts__CLIENT_PACKETS:` Trace all packet-level activity for the specified IPs.
  - `LCEfgts__CLIENT_REGISTER:` Trace all client registration changes (login, logout, disconnect, etc.) for clients coming from specified IPs.
  - `LCEfgts__EVENT1_FIELD:` Trace all clients-sent events whose `event1` field equals one of the specified strings.

- Extensive tracing of filters and alerts enforced by TASL engine now available, to facilitate troubleshooting of custom plugins.
- Added `--sort-by-rowid` option to the `list-clients` utility.

Resolved Items:

- Utility `migrateDB-toES` fails to properly delete 4.8.x silos on command.
- Configuration maladjustment possible when resetting active DB path from web UI.
- Alarming tracelog message emitted by several utilities at shutdown.
- Daemon `lce_queryd` terminates abnormally if encounters archive snapshots with extended-format filenames.
- Daemons `lced` and `lce_queryd` may terminate abnormally if archive DB is stored on a CIFS-mounted filesystem.
- Corrupt data output by `lce_client_manager -D`, under certain conditions.
- Utility `migrateDB-toES` shows a confusing interactive prompt.
- Malformatted data output by `es-helper-scripts/archival --show`, if host timezone is not GMT.

File Names & MD5 Checksums

File	MD5
lce-5.0.4-el5.x86_64.rpm	7c5c45d432094787e0d2023342e8435e
lce-5.0.4-el6.x86_64.rpm	591a87e3165005198c76f57b7bc4302c
lce-5.0.4-el7.x86_64.rpm	f24bf2f2c23db487a97c7c49d2e15fcd

Log Correlation Engine 5.0.5 Release Notes - 5/8/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

The following note describes the change that is included in Log Correlation Engine (LCE) version 5.0.5.

Resolved Items:

- File ownership issue causes `lce_www.service` to exit, preventing the web GUI from loading.

File Names & MD5 Checksums

File	MD5
lce-5.0.5-el5.x86_64.rpm	2f48c2716f0e793a3603938a4ca9a8b8
lce-5.0.5-el6.x86_64.rpm	b7ebd3e9d038bfd5a096b251295f9d96
lce-5.0.5-el7.x86_64.rpm	31f717e04910ea9fe6fb116cc9f37cec

2017 Tenable Log Correlation Engine

Log Correlation Engine 5.0.0 Release Notes - 1/31/2017

Log Correlation Engine Windows Client 5.0.0 Release Notes - 1/31/2017

Log Correlation Engine 5.0.1 Release Notes - 4/17/2017

Log Correlation Engine 5.0.2 Release Notes - 8/14/2017

LCE Windows Client 5.0.1 Release Notes - 10/30/2017

Log Correlation Engine 4.8.3 Release Notes - 10/30/2017

Log Correlation Engine 5.0.0 Release Notes - 1/31/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 5.0.0, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 5.0 User Guide.
- Supported upgrade paths:
  - 4.6.x > 5.0.0
  - 4.8.x > 5.0.0

Compatibility Notes

- LCE version 5.0.0 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 5.0.0 without issues, but will not support some new features.
- LCE version 5.0.0 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 5.0.0.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	SHA256	MD5
lce-5.0.0-el5.x86_64.rpm	7d1d32d5d741cfd32e0cc00e83e524d6025b810138155d322e2b93ae5bfcdb6d	f85ed7a4dad9eee65ab7860747aab73f
lce-5.0.0-el6.x86_64.rpm	96ee009adb43b0e06c00053c232aa140d5119047af0df172871a6d2ffb31a11e	42b456b5808201405874834 9e8c186d5

File	SHA256	MD5
lce-5.0.0-el7.x86_64.rpm	14a64016ab55272b33cc11d00b31f01e6f175190f7e45b382685051f07a1d1cc	ba59815da109f3e4908819a589290b78

New Features:

- Added support for receiving, storing, and querying Unicode characters via syslog and the LCE Windows Agent 5.0.0
- Replaced backend database with Elasticsearch to increase scalability and flexibility
- Added an Event Rule editor to simplify immediate alerting, forwarding, and filtering capabilities

Improvements:

- Improved clarity of Health and Status / Advanced reporting by adding active/archive database sizes on disk and oldest event reporting to show the timeframe covered by each database
- Improved configuration of database usage in Configuration / Storage by allowing users to directly specify the maximum space allowed to be used by LCE for the active/archive databases
- Clarified debug log options in Configuration > Advanced
- Simplified client configuration by preserving column selection and sort options after refresh and update
- Simplified client policy management by adding a "Hide Default" policies button to show only user-defined policies
- Added sub-second precision to event timestamps
- Reduced overhead in processing UDP syslog payloads on RHEL / CentOS 6 and 7 systems
- Greatly increased application data collected in debug files

Removed Features:

- Native load balancing and high availability are no longer supported. Elasticsearch should instead be leveraged for scalability with LCE 5.0.0.

Security Enhancements:

- Updated OpenSSL to 1.0.2k
- Updated libcurl to 7.52.1
- Updated jQuery UI to 1.12
- Added a lockout for administrator users after 5 unsuccessful password guesses
- See advisory TNS-2017-02 for more details

Resolved Items:

- Fixed an issue where client policies were truncated in some cases when creating client assignment rules in Configuration > Advanced

Log Correlation Engine Windows Client 5.0.0 Release Notes - 1/31/2017

The Log Correlation Engine Windows Client 5.0.0 is now available. This release contains the following changes:

New Features and Improvements:

- Added the capability to monitor Unicode text files and Unicode NT Event Logs
- Added support for DHCP so agent hosts whose IPs are dynamic will maintain the same policy, sensor name, and authorization status
- Added native client-side filtering of specific NT Event Logs by event ID and source
- Removed the .NET requirement for installation
- Switched from MD5 checksums to SHA256 for file integrity monitoring and change detection

Security Enhancements:

- Updated OpenSSL to 1.0.2k
- Updated zlib to 1.2.8
- Updated libxml2 to 2.9.4
- See advisory TNS-2017-02 for more details

Issues Addressed:

- Fixed an issue where client logins could fail if the LCE server was restarted during the login process
- Fixed a race condition between threads monitoring files and the communications thread

File Names & MD5 Checksums

File	SHA256	MD5
lce_client-5.0.0-windows_2008_x64.msi	1c8355dccdb94b4f072101e7e99212986e2ca470f5ec98ffb5aab28a473d032c	f5a54a3fcd3b0ac19244d877ccb0c9a4
lce_client-5.0.0-windows_2008_x86.msi	42c389df354b7ebe758006099665d88246b1d247587271d065cb63ab7015ca58	0f209ce2fd1b167722c996671df8b090

Log Correlation Engine 5.0.1 Release Notes - 4/17/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 5.0.1, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

Caution: If you are upgrading to LCE 5.0, review the increased hardware requirements. LCE 5.0 requires a minimum of 2x your licensed storage space, 16GB of RAM, and a 64-bit, 8-core, 3GHz processor. However, your actual hardware requirements will vary based on the number of events your LCE server is processing.

f the system running your current LCE is operating near or at maximum capacity, you should not upgrade o LCE 5.0 until ensuring the hardware requirements are met.

General Upgrade Notes

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Before upgrading from LCE Server 4.x to 5.x, please review the updated hardware requirements in the Log Correlation Engine 5.0 User Guide.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 5.0 User Guide.
- Supported upgrade paths:
  - 4.6.x > 5.0.1
  - 4.8.x > 5.0.1

Compatibility Notes

- LCE version 5.0.1 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 5.0.1 without issues, but will not support some new features.
- LCE version 5.0.1 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 5.0.1.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	SHA256	MD5	SHA1
lce-5.0.1-el5.	ebc07819c2d5148a5aa140c28a41b3cf5784d04b	17b23a8a7c6cdb5eac247a6ce2a6912c	N/A

File	SHA256	MD5	SHA1
x86_64.rpm			
lce-5.0.1-el6.x86_64.rpm	46614d8e463b1781ba3bc295ea1e970782c1fc4b73141416a01aa96cd4849d42	c76e4010e50fe80547fd4cc5b14599cc	N/A
lce-5.0.1-el7.x86_64.rpm	1c6b8b7f4c94cda80d67a4f68277fe54b5309c98	eed00f7c8fbea54ed42d2be89e533028	N/A
LCE-Server-HyperV-5.0.1-APP-LQV-	5f7b9bab98a1bb13e47e31b2a10c6087c13c3cf20d342031ddec59699d5aca64	f7ba8d4e7cbc26ee5fb7e97b24aa3d1f	dd04a85efffa44d830c3e5e5c91a995f3cfaaabb

File	SHA256	MD5	SHA1
48.zip			
LCE-Server-VMware-5.0.1-APP-LQV-48.ova	c4d7a20376129b62ceaa2e0a944c4d5b97fb431cb8d88d5e4d3b75b4920d8f5b	746801f0337342273d40abd900be29b3	46e6801ea3c17d4364dc24753bf9442018cc5aea

Improvements:

- Added a re-indexing function that allows users to re-process an index of data using the current plugin set. For usage, run /opt/lce/tools/re-indexer
- Removed case sensitivity from the user search filter
- Raised TASL virtual machine memory by 25% to 100 MB per script
- Removed 3DES from the list of supported ciphers on tcp port 1243
- Updated the LCE logo
- Ensured that the LCE logo would be visible for users using a high-contrast theme with Internet Explorer

Security Enhancements:

- Updated libcurl to 7.53.1

Resolved Items:

- Fixed a search issue where normalized queries with wildcards returned no results, or port filters could return incorrect results
- Fixed a reporting issue where non-aggregate CSV reports with more than 10,000 events would contain multiple headers embedded within the reports
- Fixed a migration issue where some events would fail to migrate to Elasticsearch from the legacy database format
- Fixed an issue where some users could not change the archive directory via the UI
- Fixed an issue where the TASL service would stop unexpectedly
- Fixed a normalization issue where a user could be unnormalized even if a plugin extracted a user substring
- Fixed a file descriptor leak on restart
- Fixed a client management issue that could cause a server to restart
- Fixed an issue where the http_proxy and ~/.curlrc files were not ignored during Elasticsearch setup

Log Correlation Engine 5.0.2 Release Notes - 8/14/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 5.0.2, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

> **Caution:** If you are upgrading to LCE 5.0, review the increased hardware requirements. LCE 5.0 requires a minimum of 2x your licensed storage space, 16GB of RAM, and a 64-bit, 8-core, 3GHz processor. However, your actual hardware requirements will vary based on the number of events your LCE server is processing. If the system running your current LCE is operating near or at maximum capacity, you should not upgrade to LCE 5.0 until ensuring the hardware requirements are met.

General Upgrade Notes

Note: If your upgrade path skips versions of Tenable Log Correlation Engine®, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Before upgrading from LCE Server 4.x to 5.x, please review the updated hardware requirements in the Log Correlation Engine 5.0 User Guide.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 5.0 User Guide.
- Supported upgrade paths:
  - 4.6.x > 5.0.2
  - 4.8.x > 5.0.2

Compatibility Notes

- LCE version 5.0.2 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 5.0.2 without issues, but will not support some new features.
- LCE version 5.0.2 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 5.0.2.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	SHA256	MD5	SHA1
lce-5.0.2-el5.x86_64.rpm	a53f26b57dea88cb669395d6b28c640f535f2a6e610ac7288a5ef4d5701a8cde	908924e27383a28cbc4e93c9e0598cb6	N/A

File	SHA256	MD5	SHA1
lce-5.0.2-el6.x86_64.rpm	96d3a8ab8126776a0de5be18e0ecf210c9efdd1422a911e5af9b11b9429784c8/td>	4e4d4384bdd833cbd79d0f8fd3a24cd7	N/A
lce-5.0.2-el7.x86_64.rpm	705ab467b65f612af83da177c43d284073afe646b344de6f37c0937488d81e96	0d9dde7b24b24bb5948df8d6b3b071ca	N/A

Improvements:

- Improved install/upgrade robustness by checking more minimum requirements, ensuring group/user creation is successful in hardened environments, adding resilience to Elasticsearch failures, preventing OS VM fragmentation when Elasticsearch starts, and fixing Bash compatibility issues for users on older systems
- Added more resolution to disk space display in the Status UI
- Deprecated options from older installations are now hidden in the Configuration UI
- The normalized Sensor field is now available to TASL scripts
- Added more information to diagnostics files related to troubleshooting installation issues
- Improved visibility for username link selection and interaction for accessibility purposes

Security Enhancements:

- Updated OpenSSL to 1.0.2l

Resolved Items:

- Fixed a resource leak in the TASL engine
- Fixed an issue where event searches could cause the Query service to consume too much CPU

- Fixed an issue where event searches with more than 1024 clauses would degrade Query performance
- Fixed an issue where, on RHEL 7 systems, LCE may not start automatically after reboot
- Fixed an issue where event searches by Asset could return more or fewer results than expected
- Fixed an issue where syslog forwarding via the Event Rules feature caused additional characters and an additional syslog header to be prepended to logs already containing a syslog header
- Fixed an issue where directional filters did not filter results as expected
- Fixed an issue that could cause corrupt sensor names in logs from LCE Agents
- Fixed an issue that could cause the engine to restart if an LCE Agent IP address changes via DHCP if other rare circumstances were met
- Fixed an issue that could cause the engine to restart if LCE internal events were created under certain circumstances
- Fixed an issue where the TASL event count function returned zero in some scripts
- Downgraded client IP changes from Alert severity to Debug severity to reduce Alert notifications in the LCE UI
- Fixed an issue where Data Sensors timestamp display dates would be significantly older than the correct date

LCE Windows Client 5.0.1 Release Notes - 10/30/2017

The following notes describe the changes that are included in Log Correlation Engine (LCE) Windows Client version 5.0.1, significant enhancements to LCE, and information about upgrading.

General Upgrade Notes

- Added the ability to throttle change reporting to reduce CPU usage in environments monitoring frequently changed files
- Added the ability to exclude directories while recursively monitoring directories for file hash changes
- Security improvement - update OpenSSL to version 1.0.2l (latest version in 1.0.2 LTS series)

- Fixed an issue where file change events are triggered when a policy is changed even if the underlying files are not changed

Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	SHA256	MD5	SHA1
lce_client-5.0.1-windows_2008_x64.msi	a3cb223cc4d292daed36797bd80b7452e6dbf535b6d9398e9f6272cadb5339aa	ba375a269fbcbb669a7c2905e0e6730c	N/A
lce_client-5.0.1-windows_2008_x86.msi	759085a3138d681bb527fc772d42cf1e01f90d8e36afe0cbbfeeba0d6a784fb0	34168cd7548a890c2d2a9eeacefa73eb	N/A

Log Correlation Engine 4.8.3 Release Notes - 10/30/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.8.3, significant enhancements to LCE, and information about upgrading.

Improvements:

- Added Targeted IDS support for SourceFire version 6.2
- Improved input validation of LCE login username field to prevent potential application issues caused by invalid characters
- Continued improvements to LCE memory usage
- Added better controls to mitigate password guessing attacks - admin account will be locked out after 5 unsuccessful login attempts
- Raised TASL VM limit to 100 MB each, allowing TASLs to store more temporal information for correlation
- Exposed sensor name to TASL scripts to allow users to pivot on the host / sensor name rather than relying only on IP addresses when TASLs are triggered

Security Enhancements:

- Upgraded cURL/libcurl to version 7.56.1 to apply the latest security updates
- Disabled 3DES cipher in LCE web server
- Updated OpenSSL to version 1.0.2l

Resolved Items:

- Fixed an issue where duplicate data sensor information and wrong timestamps were appearing in client and syslog sections of the LCE web UI
- Fixed an issue that could cause the disk to fill with TASL abort log messages
- Fixed a High Availability issue which could prevent the backup LCE server from taking over if primary server is brought down
- Fixed an issue that caused the LCE daemon to restart with the 'Unable to reload the policy map' error
- Fixed an issue that resulted in errors during processing of multiline attribute values in LCE policies and rendered the policy invalid
- Fixed an issue where policy entries in Client Assignment Rules were being truncated if multiple client policies were added to a rule

- Fixed an issue that could cause LCE to restart if plugins are reloaded while processing certain data
- Fixed an issue that was causing the 'Next Step' button to be disabled on the Quick Setup Port Configuration page
- Fixed intermittent LCE crashes caused by stopping of lce_tasld process
- Stopped addition of duplicate syslog headers, when forwarding data via UDP or TCP event forwarding rules

File Names & MD5 Checksums

File	SHA256	MD5	SHA1
lce-4.8.3-el5.x86_64.rpm	68a1c9501db6b33b7bb438fd4075017d13afdbbe86a056256e52e850dd93de9d	45f6f619ee9d13172df0ac626131d9eb	N/A
lce-4.8.3-el6.x86_64.rpm	6db24c59a6c3de728622e6dabb0277e0935df7a1174b51764913d5c5f44ba344	dc32111361dbc06ead3cc29fa3c964d6	N/A
lce-4.8.3-el7.x86_64.rpm	c5495e940daf6465f3fb70380100e5b03410e20bcef6c37517fde4438131549f	81d2f95c2b1ce2d585af6a437cc10d37	N/A

2016 Tenable Log Correlation Engine

Log Correlation Engine Splunk Client 4.6.0 Release Notes - 3/17/2016

The Log Correlation Engine Splunk Client 4.6.0 is now available. This release contains the following changes:

New Features

- Expanded configuration options allow customers to streamline and ease the burden of setup. LCE works in conjunction with Splunk to maximize a customer's security investment. This new functionality will allow users to ingest multi-line Windows logs and have them processed through the LCE engine.
- LCE can now read and write the Tenable asset GUID in conjunction with a credentialed Nessus scan for DHCP support.

Improvements

- Fixed an issue where whitelisted hostnames were only resolved at initialization time rather than upon connection. This could have resulted in whitelisting the incorrect Splunk host, or rejecting a correct Splunk host, if the DNS lookup for a whitelisted hostname changed in that time frame.

Compatibility Notes

- Splunk Client 4.6 is compatible with LCE 4.6 and later.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce_splunk-4.6.0-el6.x86_64.rpm	7eac967d84684896a720bbbbcc02d261
lce_splunk-4.6.0-el7.x86_64.rpm	4be211f45b5795da1a75bf9f8a3e7bf9

Log Correlation Engine 4.8 Release Notes - 3/17/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.8, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.8 User Guide.
- The supported upgrade path to 4.8.0 is 4.6.1, 4.6.0, and 4.4.x. If you have deployed LCE < 4.4.x, please perform an intermediate upgrade to LCE 4.4.x, then upgrade to LCE 4.8.0.

Compatibility Notes

- LCE version 4.8 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.8 without issues, but will not support some new features.
- LCE version 4.8 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 4.8.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce-4.8.0-el5.x86_64.rpm	8d1ae0900d461fd593b4daf67ee72e00
lce-4.8.0-el6.x86_64.rpm	feee53b5b38fc3d6f5459a5eb76b817d
lce-4.8.0-el7.x86_64.rpm	dc5c0830e1c05e35160407c0ffc85204
LCE-Server-HyperV-4.8.0.zip	0128d7dc4d7d1301fee9617a80aa6f3e
LCE-Server-VMware-4.8.0.ova	05baf7c763c461847a5dc2dc5185c213

New Features and Improvements:

- **LCE Client Management UI**: LCE server 4.8 can manage clients that report data to it. The new Client management UI allows users to use the LCE server as a one stop shop for all client management options. Users can assign policies, rename clients, and authorized and delete clients all from the same screen. Multi-LCE organizations may manage clients locally via the LCE UI without using SecurityCenter.
- **LCE Client Policy Editor**: The new Client policy editor guides users in creating and editing client policies. The policy editor provides a complete listing of LCE clients and allows customers to configure policy and options for all clients. The policy wizard walks users through policy modifications by showing all possible options for the selected client type, and validating them on-the-fly using a simple editor that requires no knowledge of the format of the policy. Advance users may still use the adjacent XML editor to edit the raw policy contents, if desired.
- **CVSS 3.0 Support**: LCE now supports and scores select vulnerabilities based on CVSS 3.0 rating system. This is for a limited number of vulnerabilities and may affect some dashboards and reports

Security Enhancements:

- Added configuration option to limit communication to TLS 1.2 only
- Replaced SHA1 certificate chains with SHA256
- Updated hash algorithm for completed silo from MD5 to SHA256
- Updated OpenSSL to version 1.0.2g
- Addressed CVE-2015-8035, upgraded Libxml to 2.9.3

Resolved Items:

- Segfault occurs when starting the LCE server, indexer, and TASL demons due to an issue in the config library
- LCE Server SYN Flooding
- Event rule filter “+Text” not filtering as expected
- LCE low priority queries execute slowly or not at all
- LCE- NDB Indexer will not attempt to index gzipped silos
- LCE and stats daemons not being shut down on reboot or shut down

- LCE reindex_db_elements: ERROR: unable to translate type 254
- LCE refuses to normalize usernames with inferred IPs
- TASL daemon does not attempt to read .ndb.gz files

Log Correlation Engine 4.8.1 Release Notes - 9/7/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.8.1, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.8 User Guide.
- Supported upgrade paths:
  - 4.6.0 > 4.8.1
  - 4.8.0 > 4.8.1

Compatibility Notes

- LCE version 4.8.1 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.8 without issues, but will not support some new features.
- LCE version 4.8.1 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 4.8.1.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce-4.8.1-el5.x86_64.rpm	51b91a3cdeadf800f899729a9b6b29ff

File	MD5
lce-4.8.1-el6.x86_64.rpm	e37efe41df0d7172e34c514f87dcec78
lce-4.8.1-el7.x86_64.rpm	081e931cafc3f8598cca4cd9e33fbc52

New Features and Improvements:

- Added support for Google Pub-Sub endpoints in the LCE Web Query 4.8.0 agent
- Speed up upgrades by distinctly correcting only database files and folders not already owned by LCE
- Enable extraction of usernames from plugins normalizing logs of type "login-failure"
- Reduce TASL script log file size by de-duplicating similar and adjacent admin log messages
- Log license updates in the web server log file whenever plugins are updated

Security Enhancements:

- Upgrade OpenSSL to 1.0.2h
- Upgrade libpcre to 8.39
- Upgrade libxml2 to 2.9.4
- Upgrade libcURL to 7.50.1
- Upgrade jQuery Core to 2.2.4

Resolved Items:

- Fixed a performance issue related to connecting thousands of agents to a single LCE server
- Fixed an issue rebuilding raw logs within the TASL engine which could result in incorrect tokens in rebuilt logs being passed to TASL scripts
- Fixed an issue with blank lines being sent between logs to the 2nd-to-Nth TCP syslog forward targets
- Fixed an issue where a large user database could result in a server reboot at startup
- Fixed an issue displaying IP addresses in little-endian byte order in the Connection Summary in SecurityCenter

- Fixed an issue that resulted in incorrectly interpreted included networks for some TASLs resulting in incorrect directionality calculations
- Fixed an issue where the text indexer would re-index from the first silo rather than the state persisted to disk on shutdown
- Fixed an issue where a PRM plugin with a dynamically determined event field could restart the engine
- Fixed resources leaks in the TASL engine when reloading plugins

Log Correlation Engine Web Query Client 4.8 Release Notes - 9/7/2016

The Log Correlation Engine Web Query Client 4.8.0 is now available. This release contains the following features:

Compatibility Notes

- Compatible with LCE Server 4.8.1+
- Compatible with SecurityCenter 5.1+
- All upgrade paths from prior versions of the Web Query Agent are supported

Features

- Added support for monitoring Google Cloud Platform events via Pub/Sub subscriptions to import logs directly into LCE.

File Names & MD5 Checksums

File	MD5
lce_webquery-4.8.0-el6.x86_64.rpm	035248ee9a6f0105b16cb5448c4458d0

Log Correlation Engine 4.8.2 Release Notes - 12/21/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.8.2, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.8 User Guide.
- Supported upgrade paths:
    - 4.6.x > 4.8.2
    - 4.8.x > 4.8.2

Compatibility Notes

- LCE version 4.8.2 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.8.2 without issues, but will not support some new features.
- LCE Server 5.x is compatible with all Clients.
- LCE Server 4.8.x is compatible only with LCE Client 4.x.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce-4.8.2-el5.x86_64.rpm	f7cdbc9767dd08844a47d7e4f0313393
lce-4.8.2-el6.x86_64.rpm	44bff90a989884c717f89ae24e53966b
lce-4.8.2-el7.x86_64.rpm	96e5e9cb821303c141702a80999efa37

New Features and Improvements:

- Added configuration backup and restoration scripts to /opt/lce/tools/
- Added hardware information to the debugging file
- Added bounds to the memory and host information consumed by the stats service

- Added SQLite3 pragmas for safer synchronous access to configuration, status, client, alert, and plugin databases
- Clarified workflow in the quick setup UI to guide users to enter a code and "Apply" it, or explicitly "Skip" that step

Security Enhancements:

- Updated OpenSSL to 1.0.2j
- Updated libcURL to 7.51.0
- Updated SQLite3 to 3.15.2

Resolved Items:

- Fixed an issue that caused installs to fail and report proxy services to fail to start after the RHEL 7 host was patched with glibc-2.17-157.el7
- Fixed an issue where vulnerability severity values for some plugins were invalid
- Fixed an issue where processing plugin updates could crash the web server
- Fixed an issue where the TASL service did not reinitialize if include or exclude networks were reconfigured
- Fixed an issue where processing certain logs with a certain user database could restart the log engine
- Fixed an issue where normalized database indexing could stop due to a race condition
- Fixed an unbounded memory consumption issue in the query service when using the text search filters
- Fixed an issue where Assets with zero IP addresses had incorrect event counts in the Asset Summary screen of SecurityCenter
- Removed excessive log spam when parsing the user tracking database
- Removed from the UI syslog sensors that have not received data within the past two weeks
- Fixed a UI issue where the "Override Sensor Name" feature could not be toggled and saved

2015 Tenable Log Correlation Engine

Log Correlation Engine OPSEC Client 4.4.0 Release Notes - 2/3/2015

Log Correlation Engine OPSEC Client 4.4.0 Release Notes - 2/3/2015

The Log Correlation Engine OPSEC Client 4.4.0 is now available. This release contains the following changes:

New Features

- Added the ability for the OPSEC client to be authorized and managed centrally from the LCE server using an LCE Client Policy
- Added support for all logged firewall events (previous version supported ICMP, TCP, and UDP protocol events with actions accept or drop)
- Added support to forward events directly from the client to a 3rd-party UDP syslog server
- Added the ability to optionally bind to a specific local IP when communicating with the LCE server

Bug Fixes and Improvements

- Improved logging by allowing users to configure log verbosity
- Fixed an issue where the client would be considered "Dead" by the server if polling for events took a considerable amount of time
- Fixed an issue where the OPSEC Client could exit if it was run from an environment with a long PATH environment variable value

File Names & MD5 Checksums

File	MD5
lce_opsec-4.4.0-el6.x86_64.rpm	00018561e63e7f53ed9394c049dcb8a8

Log Correlation Engine Client 4.2.1 for Red Hat EL 5.0 and 6.0 Release Notes - 2/16/2015

The Log Correlation Engine Client 4.2.1 for Red Hat EL 5.0 and 6.0 is now available. This update fixes an issue where files newly whitelisted in the malware DB would be falsely reported by the LCE client as malware according to "0 AVs".

File Names & MD5 Checksums

File	MD5
lce_client-4.2.1-el5.i386.rpm	d240f1de9899901b80dfd65ccfb7acd3
lce_client-4.2.1-el5.x86_64.rpm	6a2b6a64fe3c16e235b4e0e14a02ab06
lce_client-4.2.1-el6.i386.rpm	724f9852b841e341da988535632bdeb6
lce_client-4.2.1-el6.x86_64.rpm	2b1dd2877c3e00a8b0094183d78b5e24

Log Correlation Engine 4.6 Release Notes - 8/20/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.6.0, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.6 Administration and User Guide.
- Prior to upgrading to LCE 4.6.0, ensure that your "Feed Expiration" is not expired and your "Activation Status" is "Licensed" by logging in to the LCE web interface, clicking on "Health and Status", then clicking on "Plugins". If these fields are not valid, then LCE 4.6.0 will cease to run until a new activation code is applied.
- The only supported upgrade path is from LCE 4.4.x to LCE 4.6.0. If you have deployed LCE < 4.4.x, please perform an intermediate upgrade to LCE 4.4.x, then upgrade to LCE 4.6.0.

Compatibility Notes

- LCE version 4.6.0 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.4.1 without issues, but will not support some new features.
- LCE version 4.6.0 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 4.6.0
- Prior to upgrading or deploying LCE 4.6.0 with High Availability, please contact Tenable Support.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce-4.6.0-el5.x86_64.rpm	77c498fa3a714aeea1da765357da21ae
lce-4.6.0-el6.x86_64.rpm	fdfd7b4bf1be3326d04f3b314475144c
lce-4.6.0-el7.x86_64.rpm	ad5f0065441d9ce4d76ed70dfc634fcc

New Features and Improvements:

Improvements

- TLS TCP Syslog: LCE can now receive encrypted reliable syslog data from verified senders.
- DHCP Client Support: LCE 4.6.0 introduces DHCP client support. LCE Clients (version 4.6.0+) can be authorized once and will be recognized even if the endpoint receives a new IP address.
- Simplified licensing: The lce.key file is no longer required; the activation code now provides the license and the plugin subscription.
- Simplified offline registration and plugin update: Follow the instructions at https://plugins.nessus.org/v2/offline-lce.php to perform offline activation and plugin updates.

Issues Addressed:

- Fixed a log engine deadlock and memory leak associated with importing statistical info-level vulnerability data every two hours
- Removed support for SSLv3 on all interfaces, removed support for TLSv1 on most interfaces, and tightened accepted cipher suites

- Fixed an issue where offline plugin updates occasionally failed
- Fixed an issue where LCE would return incorrect results to SecurityCenter if IPv6 ranges were included in a Repository

Log Correlation Engine 4.6.1 Release Notes - 12/1/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.6.1, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.6 Administration and User Guide.
- The supported upgrade path is from LCE 4.4.x to LCE 4.6.1 and LCE 4.6.0 to LCE 4.6.1. If you have deployed LCE < 4.4.x, please perform an intermediate upgrade to LCE 4.4.x, then upgrade to LCE 4.6.1.

Compatibility Notes

- LCE version 4.6.1 is compatible with SecurityCenter version 5.1 or later. Older versions of SecurityCenter will work with LCE 4.4.1 without issues, but will not support some new features.
- LCE version 4.6.1 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 4.6.1
- Prior to upgrading or deploying LCE 4.6.x with High Availability, please contact Tenable Support.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce-4.6.1-el5.x86_64.rpm	8c0eab51916a56a3506d142a9e17def3
lce-4.6.1-el6.x86_64.rpm	6752d203651a3df5a05fe3c31571946e
lce-4.6.1-el7.x86_64.rpm	05bf787561f882b51de2bc702cd871aa
LCE-Server-HyperV-20141110-1155.zip	8aefceb133da8c88b89b37628d8fad1a
LCE-Server-VMware-20160119-2330.ova	19cd0f5cbec93ef016c87845bab24cdc

New Features and Improvements:

- Added a multi-threaded option for the log_importer tool to allow faster import of large sets of data. Use "-j" or "--jobs" to specify the number of threads.
- Improved performance over LCE 4.6.0 by moving TASL processors to a separate, new TASL Engine process. The process can be monitored, started, and stopped along with other LCE Server components using the LCE UI.
- Added support for the Web Query Client.

Issues Addressed:

- Fixed an issue where a successful plugin update could cause the web server to hang.
- Fixed an issue where "Event Rules" could be cleared in the UI when modified.
- Fixed an issue that caused the Query Interface to hang if a query was performed with certain special characters in a specific order.
- Fixed an issue in the log_importer tool encountered if /opt/lce/tmp/ and the archive directory were not on the same filesystem.
- Fixed an issue where the Text Indexer could become stuck on a certain database entry.
- Fixed an issue on RHEL7 where services would not restart on reboot.
- Fixed an issue where the UI prevented re-registration from the Feed Settings page if the Activation Code was unchanged.
- Fixed a few resource leaks in the Query Interface and the Log Engine, and excessive memory usage by the lce_client_manager tool.

Log Correlation Engine Web Query Client 4.6 Release Notes - 12/10/2015

The Log Correlation Engine Web Query Client 4.6.0 is now available. This release contains the following features:

Compatibility Notes

- Compatible with LCE 4.6.1+ and SecurityCenter 5.1+

Features

- Monitor Amazon Web Services (AWS) API events via Cloudtrail, and import the events directly into LCE
- Monitor Salesforce user successful logins, failed logins, and user changes, and import the events directly into LCE
- Prevent exceeding cloud-based service limits with configurable thresholds on bytes or calls used for monitoring
- Reads and writes the Tenable Asset GUID (TAG) in conjunction with credentialed Nessus scans for DHCP support

File Names & MD5 Checksums

File	MD5
lce_webquery-4.6.0-el6.x86_64.rpm	3d5bba5502144d3f5c3efb2f59c3c99c

2014 Tenable Log Correlation Engine

Tenable Network Monitor 4.2.0 Release Notes - 1/13/2014

Log Correlation Engine Unix Client 4.2.0 Release Notes

Log Correlation Engine Splunk Client 4.2.0 Release Notes - 2/25/2014

Log Correlation Engine WMI Monitor 4.2.0 Release Notes - 3/5/2014

Log Correlation Engine NetFlow Monitor 4.2.0 Release Notes - 3/10/2014

Log Correlation Engine SDEE Monitor 4.2.0 Release Notes - 3/28/2014

Log Correlation Engine WMI Monitor 4.2.1 Release Notes - 4/2/2014

Log Correlation Engine WMI Monitor 4.2.2 Release Notes - 4/30/2014

Log Correlation Engine 4.2.2 HOTFIX lce_report_proxyd binary Release Notes - 6/9/2014

Log Correlation Engine 4.4.0 Release Notes - 8/12/2014

LCE HTML Client 1.0.1 and Web Server 1.0.1 for LCE 4.4 Release Notes - 9/29/2014

Log Correlation Engine 4.4.1 Release Notes - 10/28/2014

Log Correlation Engine Windows Client 4.4.0 Release Notes - 12/16/2014

Log Correlation Engine Client 4.2.1 for Red Hat EL 7.0 Release Notes - 12/29/2014

Tenable Network Monitor 4.2.0 Release Notes - 1/13/2014

The Tenable Network Monitor 4.2.0 is now available. This release contains the following changes:

- Implemented an unattended installation mechanism - after an installation, the set-server-ip.sh can be used to automatically configure the LCE server IP/hostname/port and start the LCE Client.
- Fixed a packaging issue where the client could be installed on the incorrect architecture and no traffic would be captured.

File Names & MD5 Checksums

File	MD5
TenableNetworkMonitor-4.2.0-el5.i386.rpm	b758c3dcc197bbf2b3a43d9225d5ca8c
TenableNetworkMonitor-4.2.0-el5.x86_64.rpm	02b25646641980e5d4dcaa53d189eb3c
TenableNetworkMonitor-4.2.0-el6.i386.rpm	eef7052dac87a816d12f8bc7bfe53792
TenableNetworkMonitor-4.2.0-el6.x86_64.rpm	47127fbed50a783e618b713834716ebc

Log Correlation Engine Unix Client 4.2.0 Release Notes

The following Log Correlation Engine Unix 4.2.0 clients are now available:

File Names & MD5 Checksums

File	MD5
lce_client-4.2.0-AIX.bff	df6eea645aea78092e5ecc2bf67016ca
lce_client_4.2.0_debian6.i386.deb	de3d0007be3db4dd6f2cced6aa9797bd

File	MD5
Ice_client_4.2.0_debian6.x86_64.deb	31bcbd034024fa7f3f61a04c9990f342
Ice_client_4.2.0_debian7.i386.deb	953cd509b22a3cb280544338befd1705
Ice_client_4.2.0_debian7.x86_64.deb	c914ad1129e49f4642cbacc4c79d0c53
Ice_client-4.2.0-el5.i386.rpm	757d51c5b6d31a6af5738c87d631e2e1
Ice_client-4.2.0-el5.x86_64.rpm	8a5732b5bddc08857df664bbd426117f
Ice_client-4.2.0-el6.i386.rpm	93b88dca99a253dd25f540fefd736342
Ice_client-4.2.0-el6.x86_64.rpm	cab879f33b885adba1116c926b5f8538
Ice_client-4.2.0-fedora18.i386.rpm	16e2ca61f871b01f12934b02b43e1eae
Ice_client-4.2.0-fedora18.x86_64.rpm	83994464574ebbdba57b722ee7a16d07
Ice_client-4.2.0-fedora19.i386.rpm	fe10cbab66a0cb3411be88a9f96e7ad6
Ice_client-4.2.0-fedora19.x86_64.rpm	5359a4e6ee77c17c194f901297eef793
Ice_client-4.2.0-freebsd8_amd64.tbz	7aadb5374c6a8f5f1bdfa1c7f43b5267
Ice_client-4.2.0-freebsd8_i386.tbz	56520d87b9e9314077ba42a9f61d7bd7
Ice_client-4.2.0-freebsd9_amd64.tbz	faa6df0bba6a4bd1be39cd1ab006505b
Ice_client-4.2.0-freebsd9_i386.tbz	40b0e230a217fadcd06523c5ab01a1a2
Ice_client-4.2.0-Itanium.depot	21d228c2a09aa7f96bb5499234ef0ff0
Ice_client-4.2.0-RISC.depot	478239056681d5f7213629b3e717d245
Ice_client-4.2.0-osx.pkg.tar.gz	96c830dbef89dd7d7c921af92cc59be2
Ice_client-4.2.0-SPARC.pkg.tar.gz	12c3994a427537f8c596463b049f2d39
Ice_client-4.2.0-suse11.i586.rpm	445fd678f863208b186ce9a5b2986261
Ice_client-4.2.0-suse11.x86_64.rpm	d1fd37fcc969ae9deac5a131e9c07b5c
Ice_client_4.2.0-ubuntu13_i386.deb	e7cd4d2e1e2161e606a3c167ad79c2f7

File	MD5
lce_client_4.2.0-ubuntu13_x86_64.deb	c88618079467792b6ca825c3b357c711
lce_client_4.2.0-ubuntu12_i386.deb	80c85e0c24b906b59644486b517a4600
lce_client_4.2.0-ubuntu12_x86_64.deb	131ab06e2e86eed06a4da1b792f5c617

This release contains the following changes:

New features:

- Malware Scanning: The LCE client will scan running processes regularly for malware, similar to Nessus. For details on how to enable and configure this capability, please refer to the LCE Clients Guide (Malware scanning is not supported on the AIX and HP-UX clients).
- If the LCE Client is configured to monitor process accounting logs but process accounting is not enabled, the LCE Client will attempt to enable it on the host during startup.
- Implemented an unattended installation mechanism - after an installation, the set-server-ip.sh can be used to automatically configure the LCE server IP/hostname/port and start the LCE Client.

Bug fixes:

- Fixed an issue that could cause clients to fail to send events or reconnect to the LCE server after a certain number of LCE server restarts.
- Fixed the content displayed in the network statistics log.
- Fixed an issue where new directories created under "recursive-directory-changes" tags were not rescanned.
- Fixed a memory leak that could occur if a certain misconfiguration was encountered in the LCE Client policy.

* Policy assignments and modifications for the SuSE LCE Client must be performed directly with the lce_client_manager on the LCE Server host rather than SecurityCenter.

Log Correlation Engine Splunk Client 4.2.0 Release Notes - 2/25/2014

The Log Correlation Engine Splunk Client 4.2.0 is now available. This release contains the following changes:

- Upgraded the LCE Splunk Client to utilize the centrally-managed LCE Client Policy (.lcp) files for configuration in lieu of lce_splunk.conf
- To convert lce_splunk.conf to a LCP file, please see the LCE Client Guide section labeled "LCE Conf Converter"
- To learn more about centrally-managed LCE Client Policies, please see the LCE Client Guide section labeled "LCE Client Manager"

File Names & MD5 Checksums

File	MD5
lce_splunk-4.2.0-el5.i386.rpm	b9d38a7d63172a124716deab399d53f1
lce_splunk-4.2.0-el5.x86_64.rpm	217d4eba1efc3e7dce14e698127ddc0f
lce_splunk-4.2.0-el6.i386.rpm	adb61dc4373c9c70e12d4b98ccb68224
lce_splunk-4.2.0-el6.x86_64.rpm	49788431406b4cfa46b22ba9e8e19298

Log Correlation Engine WMI Monitor 4.2.0 Release Notes - 3/5/2014

The Log Correlation Engine WMI Monitor 4.2.0 is now available. This release contains the following changes:

New Features

- Added support for a set of "default" credentials. These credentials will be used by the WMI Monitor for all monitored hosts that do not have their own explicit credentials specified. Please use /opt/wmi_monitor/wmi_config_credentials to generate these credentials.
- Added a per-host time window that now tracks a monitored host when it disconnects from, then reconnects to, the network to receive logs stored on that host while it was off of the network. A new configuration element "delta-time-frame-cap" limits the size of the query window, in seconds.

Bug Fixes and Improvements

- Removed the legacy configuration wmi_monitor.conf file from new distributions and added set-server-ip.sh for easily configuring the client to connect to the LCE server.

- Improved robustness of policy update procedure that could cause issues previously if the policy changed while monitoring large numbers of hosts.
- Improved handling and logging of monitored hosts in different time zones.
- Fixed an issue where a policy was considered valid with an invalid IP or hostname.
- Fixed an issue where monitoring a large number of offline hosts would result in a delayed login with the LCE server.

File Names & MD5 Checksums

File	MD5
wmi_monitor-4.2.0-el5.i386.rpm	17d6d26e220a615f3a29ef43f1462524
wmi_monitor-4.2.0-el5.x86_64.rpm	514219646867dd49a0a9d6183e469f6a
wmi_monitor-4.2.0-el6.i386.rpm	a61b20825d3a935b3f2eb96cb0bcee61
wmi_monitor-4.2.0-el6.x86_64.rpm	a9c596e56a67b570808687ae80c1382c

Log Correlation Engine NetFlow Monitor 4.2.0 Release Notes - 3/10/2014

NetFlow Monitor 4.2.0 is a maintenance update with a few bug fixes and new features.

New Features:

- Added support for IPFIX (v10) IPv4 records and templates
- Added support for AppFlow IPv4 records and templates - the application name, if available, is available at the end of the raw syslog message generated by the NetFlow Monitor
- Added de-duplication logic to handle matching flow records from different flow sources

Bug Fixes and Improvements:

- Resolved a memory consumption and stability issue when monitoring NetFlow v9

File Names & MD5 Checksums

File	MD5
TenableNetFlowMonitor-4.2.0-el5.i386.rpm	2c4e54e08fb920e9351633f7c0328bc6
TenableNetFlowMonitor-4.2.0-el5.x86_64.rpm	7ae6fdc4f50fae453fed9f44a5f65951

File	MD5
TenableNetFlowMonitor-4.2.0-el6.i386.rpm	194461b21044ce0e631036510fa809f6
TenableNetFlowMonitor-4.2.0-el6.x86_64.rpm	42ea6f1fb2f679e9c9573198de282b40

Log Correlation Engine SDEE Monitor 4.2.0 Release Notes - 3/28/2014

Please note: This release of the LCE SDEE Monitor coincides with the EOL of the LCE RDEP Monitor due to the EOL of RDEP itself. Users are encouraged to use the LCE SDEE Monitor to monitor security devices supporting SDEE, which supersedes RDEP. Please contact Tenable Support if RDEP monitoring support is still required on your network.

New Features:

- Upgraded the LCE SDEE Monitor to utilize the centrally-managed LCE Client Policy (.lcp) files for configuration in lieu of sdee_monitor.conf
- To convert sdee_monitor.conf to a LCP file, please see the LCE Client Guide section labeled "LCE Conf Converter"
- To learn more about centrally-managed LCE Client Policies, please see the LCE Client Guide section labeled "LCE Client Manager"

Bug Fixes and Improvements:

- Added RPM dependency upon libidn shared object library
- Added more validation to IP address and hostname fields
- Greatly improved login speed with LCE server

File Names & MD5 Checksums

File	MD5
sdee_monitor-4.2.0-el5.i386.rpm	0fa43fbdffda2972ec5a8a14a555a9a7
sdee_monitor-4.2.0-el5.x86_64.rpm	352763715442ef573a34510bb597ecb0
sdee_monitor-4.2.0-el6.i386.rpm	d81beaa4c3ceaaa6c0b82072efd4476c
sdee_monitor-4.2.0-el6.x86_64.rpm	5c19ddbe5d09e6f74e2e9b9ca32e706c

Log Correlation Engine WMI Monitor 4.2.1 Release Notes - 4/2/2014

The Log Correlation Engine WMI Monitor 4.2.1 is now available. This fixes a critical issue monitoring hosts configured to use Daylight Savings Time.

File Names & MD5 Checksums

File	MD5
wmi_monitor-4.2.1-el5.i386.rpm	5ad2592bb23a07a156551dc2e72db00f
wmi_monitor-4.2.1-el5.x86_64.rpm	ec698f168de22ee114b999beb919381c
wmi_monitor-4.2.1-el6.i386.rpm	10b40f69aa836ae75f2939197240644c
wmi_monitor-4.2.1-el6.x86_64.rpm	cc068bb272d328824681a60027a3ebad

Log Correlation Engine WMI Monitor 4.2.2 Release Notes - 4/30/2014

The Log Correlation Engine WMI Monitor 4.2.2 is now available.

Bug Fixes and Improvements

Fixed an issue where monitoring a host by hostname then disconnecting from that host could cause the WMI Monitor service to halt.

File Names & MD5 Checksums

File	MD5
wmi_monitor-4.2.2-el5.i386.rpm	188e9be3417534bc4573ee0dedfe1def
wmi_monitor-4.2.2-el5.x86_64.rpm	a4603d02a2206080fa6a69867ac6cc7f
wmi_monitor-4.2.2-el6.i386.rpm	98a9fb8df123861f624267dceb291959
wmi_monitor-4.2.2-el6.x86_64.rpm	ed1b868a0914add589620bca87a2057d

Log Correlation Engine 4.2.2 HOTFIX lce_report_proxyd binary Release Notes - 6/9/2014

This hotfix release patches the LCE Report Proxy executable in LCE 4.2.x, which used a version of OpenSSL that may have been vulnerable to CVE-2014-0224. Users are encouraged to update immediately. To patch the LCE Server, download the hotfix binary to the LCE Server host and run the following commands replacing <os> and <arch> appropriately:

```
# /sbin/service lce_report_proxy stop
# cp --preserve /opt/lce/daemons/lce_report_proxyd /opt/lce/daemons/lce_report_proxyd_422
# cp ~/lce_report_proxyd_<os>_<arch> /opt/lce/daemons/lce_report_proxyd
# chown root:root /opt/lce/daemons/lce_report_proxyd
# chmod 6750 /opt/lce/daemons/lce_report_proxyd
# /sbin/service lce_report_proxy start
```

Users upgrading directly from LCE 4.2.0 should be aware that the LCE Report Proxy now binds to the "server-address" specified in lce.conf rather than all addresses.

End users can verify successful application of this patch with the console command "/opt/lce/daemons/lce_report_proxyd -v"

File Names & MD5 Checksums

File	MD5
lce_report_proxyd_el5_i386	00d7710fd58e4cc0299a5c21b2307e5c
lce_report_proxyd_el5_x86_64	6ce1006d6a5774e5a74a8953b184708a
lce_report_proxyd_el6_i386	3ad6cd53dbfd86e4003a32bd23889349
lce_report_proxyd_el6_x86_64	4a759371025b7520bfb90b496bfe1e53

Log Correlation Engine 4.4.0 Release Notes - 8/12/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.4.0, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.4 Administration and User Guide.

- Upgrading to LCE version 4.4.0 from LCE version 3.x or earlier is not supported. An intermediate upgrade to LCE 4.2.2 must be performed before upgrading to LCE 4.4.0.
- After upgrading to LCE version 4.4.0, the text-based configuration files (e.g., lce.conf) will be migrated to a database and are no longer used.

Compatibility Notes

- LCE version 4.4.0 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.4.0 without issues, but will not support some new features.
- LCE version 4.4.0 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 4.4.0.
- Prior to upgrading or deploying LCE 4.4.0 with High Availability, please contact Tenable Support.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce-4.4.0-el5.x86_64.rpm	f36aeb548a21f16f1621893fe805acad
lce-4.4.0-el6.x86_64.rpm	73f8a5a5ffd6dc1cc799b3ffa24ce556

Application Notes

New Features

- New User Interface - a new HTML5 web-based interface similar to Nessus may now be used to configure and administer LCE.
- Streamlined Installation - to configure and setup LCE for the first time, direct your browser to https://<IP or hostname of LCE server>:8836 and follow the quick-setup instructions.
- New Syslog Forwarding - LCE can now forward events in CEF (Common Event Format) from the log engine or forward specific events in CEF using the Event Rules configuration section.
- Enhanced Sensor Reporting - the web-based interface allows users to quickly see the total number of logs sent and last timestamp for all known syslog and LCE Client data sensors.

- Automatic Client Authorization and Policy Assignment - client rules can now be set to automatically authorize and assign client policies given a client network range.

Improvements

- Increased the number of unique normalized events, detailed events, and sensors that LCE is capable of storing.
- Lowered the write operations/second of the log engine with enhanced batched normalized database writes.
- Added an override to use the network source address for all LCE Clients as the normalized source address in lieu of the reported LCE Client private address.
- Added the ability to delete a client policy using the lce_client_manager tool.

Issues Addressed

- Patched LCE Report Proxy for CVE-2013-2566. This patch was also released separately as a hotfix for LCE version 4.2.2.
- Fixed an issue where the LCE server would not shutdown if the installation directory file system or database directory file system has insufficient space.
- Fixed several issues where unnormalized events or internally generated events for load balancing, clients, and host discovery normalized the incorrect source or destination IP address.
- Fixed an issue where invalid input to the lce_client_manager could cause an LCE Client to be assigned to an LCE Server of 0.0.0.0:0.
- Fixed an issue parsing IDS events from a Snort sensor if the Snort sensor hostname contained a particular string.
- Fixed an issue where duplicate clients could be listed by the lce_client_manager tool.
- Fixed an issue where compound text queries for "verbose" returned incorrect results.
- Fixed an issue where queries for an event with "syslog" in the query returned incorrect results.
- Fixed an issue where specific IP ranges in a SecurityCenter repository could cause some IPs to be omitted from LCE event results.
- Fixed an issue where negative query filters on the port attribute returned incorrect results.

- Fixed an issue where a TASL could stop the LCE engine if it exhausted its allowed memory footprint.
- Fixed an issue where specific IDS processing may not occur if the IDS configuration between the Primary LCE and Auxiliary LCE did not match.

LCE HTML Client 1.0.1 and Web Server 1.0.1 for LCE 4.4 Release Notes - 9/29/2014

The LCE HTML Client 1.0.1 and Web Server 1.0.1 are now available. These updates will be distributed to customers via the LCE plugin feed.

Improvements:

Users may now modify the following configuration items in the LCE web interface:

- User-agent string used to identify LCE during plugin update requests
- Automated plugin update interval, in days
- Web client session timeout, in minutes
- Improved the look of the service control interface

Bug Fixes:

- Fixed text layout and text area re-size issues
- Fixed an issue where a specific expired web client session was not destroyed
- Fixed an issue where the private IP address of the web server could be disclosed (NID 10759)
- Fixed an issue displaying very long usernames.

Log Correlation Engine 4.4.1 Release Notes - 10/28/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.4.1, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

General Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.4 Administration and User Guide.
- Upgrading to LCE version 4.4.1 from LCE version 3.x or earlier is not supported. An intermediate upgrade to LCE 4.2.2 must be performed before upgrading to LCE 4.4.1.
- After upgrading to LCE version 4.4.1, the text-based configuration files (e.g., lce.conf) will be migrated to a database and are no longer used.

Compatibility Notes

- LCE version 4.4.1 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.4.1 without issues, but will not support some new features.
- LCE version 4.4.1 is compatible with LCE Clients version 4.0.0 or later. Older LCE Clients will not be able to log in and send event data to LCE 4.4.1.
- Prior to upgrading or deploying LCE 4.4.1 with High Availability, please contact Tenable Support.
- Please contact Tenable Support if you have any questions about compatibility issues.

File Names & MD5 Checksums

File	MD5
lce-4.4.1-el5.x86_64.rpm	1a8c7056a8254c4883f456d83ee5f9e8
lce-4.4.1-el6.x86_64.rpm	71d8f6e8c7c2a003599ed2e7e457a963
LCE-Server-4.4.1-HyperV.zip	e6bec0fb2902b9e605d62025f093d2c7
LCE-Server-4.4.1-VMware.ova	eacd85eb0a577eedc59d5498450d9652

Application Notes

Improvements

- Greatly enhanced indexer performance of normalized data
- Increased default RSA key length of self-generated certificate to 2048 bits

Issues Addressed

- Fixed an issue where silos did not roll at the configured value
- Patched the LCE report proxy and web server to remove SSLv3 support (CVE-2014-3566)
- Fixed an issue preventing some users from manually uploading a plugin file via the Web UI to update plugins
- Fixed an issue where an Asset Summary displayed showed incorrect event counts
- Fixed an issue where a client index could be re-used if the highest-indexed client was deleted
- Fixed an issue where upgrading to LCE 4.4.x could cause duplicate entries in some configuration tables such as Sampleable TASLs and Trusted Plugin

Log Correlation Engine Windows Client 4.4.0 Release Notes - 12/16/2014

The Log Correlation Engine Windows Client 4.4.0 is now available. This release contains the following changes:

New features:

- Added a malware check of monitored files on disk, in addition to currently monitored processes
- Added the ability to see the assigned policy filename in the configuration utility
- Added the ability to log new events from the Windows event log that were recorded when the LCE Client was not running
- Greatly enhanced the performance of monitoring a large number of files and directories for changes

Improvements and Issues Addressed:

- Significantly improved event compression in transit to reduce bandwidth used by the client
- Added an option to leave logs and data files on disk during uninstall
- Fixed an issue where MDAC was incorrectly required for installations
- Fixed a resource utilization issue if the client started and could not resolve the hostname of the LCE server
- Fixed an issue where repairing an installation could reset the assigned policy incorrectly

- Fixed an issue where all Windows event log sources may not be captured on some Windows 2003 hosts
- Deprecated "monitor-config"
- Removed Microsoft merge modules from the installation - users will need to download required Microsoft redistributables prior to installation

Notes:

- If a Windows LCE Client policy contains <event-log>Security</event-log> and at least one <monitor-file> tag, it is recommended that the Local Security Policy / Audit Policy does not audit Successful object access events. This will cause the LCE client to report every successful access of files checked by the <monitor-file> tags.

File Names & MD5 Checksums

File	MD5
lce_client-4.4.0-windows_2003_x86.msi	6abce1745725b3f9684ae27156fb97b0
lce_client-4.4.0-windows_2008_x64.msi	76eac78252f7fcef3b26118037771354
lce_client-4.4.0-windows_2008_x86.msi	988d452abbc04d6cab1eccdac1238f7e

Log Correlation Engine Client 4.2.1 for Red Hat EL 7.0 Release Notes - 12/29/2014

The Log Correlation Engine Client 4.2.1 for Red Hat EL 7.0 is now available. This release provides support for Red Hat EL 7.0 and Red Hat EL 7.0-based platforms (Oracle Linux, CentOS, and Scientific Linux).

File Names & MD5 Checksums

File	MD5
lce_client-4.2.1-el7.x86_64.rpm	aab8a19d8996ccc6e99e22bc02101af3

2013 Tenable Log Correlation Engine

Log Correlation Engine Client 4.0.1 for Mac OS X Release Notes - 2/20/2013

Log Correlation Engine 4.2.0 Release Notes - 5/23/2013

Log Correlation Engine 4.2.1 Release Notes - 8/12/2013

Log Correlation Engine Windows Client 4.2.0 Release Notes - 9/26/2013

Log Correlation Engine 4.2.2 Release Notes - 12/9/2013

Log Correlation Engine Windows Client 4.2.1 Release Notes - 12/16/2013

Log Correlation Engine Client 4.0.1 for Mac OS X Release Notes - 2/20/2013

The Log Correlation Engine Client 4.0.1 for Mac OS X now available. This release contains the following changes:

- Resolved an issue where it was possible to get an additional event per log during a policy update.
- Resolved an issue where the removal of statistics-frequency or heartbeat-frequency, or modifying these values in a policy and then updating the policy client-side, could potentially result in an inaccurate reporting frequency of heartbeat log messages or client statistic log messages.
- Resolved an issue where rapid policy changes or modifications server-side could result in the client using an outdated policy.

File Names & MD5 Checksums

File	MD5
lce_client-4.0.1-osx.pkg.tar.gz	c70b88541c060891e2920ef0589be09b

Log Correlation Engine 4.2.0 Release Notes - 5/23/2013

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.2.0, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.

- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.2 Administration and User Guide.
- Lowering the number-silos setting can impact data storage. If this setting is lowered after data has been collected, LCE will archive or delete silos ranging outside of the specified maximum when rolling to silo 0. The silo archiving settings in the lce.conf file must be enabled for data to be archived in this manner.
- LCE version 4.2 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.2 without issues, but will not support many of the new features available in LCE 4.2. Please contact Tenable Support if you have any questions about compatibility issues.
- The report proxy settings must be configured to enable LCE's new reporting features. This can be done by editing the Discovery Options section of the lce.conf file, or running the /opt/lce/tools/lce-post-install.sh script.
- LCE 4.2 must first be activated using your provided activation code for plugins and other updates to be retrieved. This can be accomplished by running the /opt/lce/tools/lce-post-install.sh post-install script.

Upgrading from LCE 3.x

- Beginning with version 4.0 LCE Clients, their configuration files, now called "policies", must be managed centrally with the LCE Client Manager tool when connected to LCE Server 4.0 or later. Existing configuration files may be converted using the LCE Configuration File Converter tool, and imported/assigned with the LCE Client Manager. LCE Clients connected to an LCE Server 3.6 or earlier may continue to use the traditional configuration files.
- The LCE log archive feature has been removed. New logs will be searchable via SecurityCenter's "Events" analysis tools.

File Names & MD5 Checksums

File	MD5
lce-4.2.0-el5.i386.rpm	[789e1bde3846b6b6739ef287cfe3b772]
lce-4.2.0-el5.x86_64.rpm	[950f5406c0632213e2f3769713a125a6]
lce-4.2.0-el6.i386.rpm	[54abcb7ee0567d417ec90bc8ac958e4e]
lce-4.2.0-el6.x86_64.rpm	[91117f0d9786021315abbbcc693eea93]

Application Notes

Major New Features

- **Automatic Asset Discovery.** Information is now extracted from log data to identify and report assets present on the network. When used in conjunction with SecurityCenter, Nessus, and PVS, this enables discovery and inventory of 100% of IT assets, both authorized and unauthorized, in any network topology.
- **Vulnerability Detection.** LCE now performs additional analysis on log data to identify and report a variety of vulnerabilities. (only available when used with SecurityCenter 4.6.2.2)
- **Advanced Network Profiling.** While log data is being processed, LCE now continually builds a detailed profile of the network to provide additional contextual data for analysis and reporting on security and compliance. The profile includes a unique list of user accounts active on each host, a collection of statistics defining the footprint of normalized logs for each host, reporting of open and browsed ports by some applications, and more. (only available when used with SecurityCenter 4.6.2.2)
- **High Availability.** A powerful set of features supporting high availability requirements has been added. This includes the ability to create a redundant remote copy of a system using a new log mirroring component, along with advanced load balancing and automated capabilities for failover and recovery. Please see the LCE High Availability Large Scale Deployment Guide for more detail. (only available when used with SecurityCenter/LCE Manager 4.6.2.2)

Other New Features/Improvements Added

- Ability to filter events by text content when defining rules in rules.conf.
- Ability to define separate source and destination IP address filters in rules.conf.
- Ability to access a log’s normalized username in TASL scripts.
- Support for Suricata IDS products. These can be added with the Snort type in lce.conf.
- A configuration option to force user-defined sensor names to override sensor names extracted from logs.
- Option to automatically authorize all clients that connect to the server during a configurable time window after LCE starts.

- Ability to reload the system configuration after changes, without the need to restart the LCE service.
- Any non-printable characters in logs are now stored with their hexadecimal representations.
- Query performance has been improved by ensuring utilization of all available CPU cores even when only processing a single query.

Bugs Addressed

- Fixed an issue that prevented vulnerabilities with critical severity from being correlated with IDS events.
- Fixed an issue that caused full text searches including very large numeric strings to fail.
- Fixed an issue that could have prevented the query daemon from recovering automatically after a failure.

Log Correlation Engine 4.2.1 Release Notes - 8/12/2013

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.2.1, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.2 Administration and User Guide.
- The LCE Server Virtual Machine Quick Start Guide explains how to initially configure the LCE server virtual machine.
- Lowering the number-silos setting can impact data storage. If this setting is lowered after data has been collected, LCE will archive or delete silos ranging outside of the specified maximum when rolling to silo 0. In order for data to be archived in this scenario, the silo archiving settings in lce.conf must be enabled.

- LCE version 4.2 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.2 without issues, but will not support many of the new features available in LCE 4.2. Please contact Tenable Support if you have any questions about compatibility issues.

Upgrading from LCE 4.0.x and below

- In order to enable LCE’s reporting features, the report proxy settings must be configured. This can be done by editing the “Discovery Options” section of lce.conf, or running the /opt/lce/tools/lce-post-install.sh script.
- In order for plugins and other updates to be retrieved, LCE 4.2 must first be activated using your provided activation code. This can be done by running the post-install script referenced above.

Upgrading from LCE 3.x

- Beginning with version 4.0 LCE Clients, their configuration files, now called “policies”, must be managed centrally with the LCE Client Manager tool when connected to LCE Server 4.0 or later. Existing configuration files may be converted using the LCE Configuration File Converter tool, and imported/assigned with the LCE Client Manager. LCE Clients connected to an LCE Server 3.6 or earlier may continue to use the traditional configuration files.
- The LCE log archive feature has been removed. Existing logs may continue to be searched via the SecurityCenter's “Raw Log Search”, but new logs will be searchable via SecurityCenter's “Events” analysis.

File Names & MD5 Checksums

File	MD5
lce-4.2.1-el5.i386.rpm	[99eb71ea14649064ff064596573c85eb]
lce-4.2.1-el5.x86_64.rpm	[c81fd7edfcb39e7ed2da1955272f4dbc]
lce-4.2.1-el6.i386.rpm	[c465f8b5ec199d4c30235be3d336dc9d]
lce-4.2.1-el6.x86_64.rpm	[99a30fa84927253ee594f8bee48fa930]
LCE-Server-4.2.1-HyperV.zip	[cf77ceefc2c6d044b0c60d9bddf3c727]
LCE-Server-4.2.1-VMware.ova	[572cfe1275cc82efe1ad4c61ce1d8bcf]

Application Notes

New Features and Improvements

- Added an option to the plugins update script to retain the plugins archive and signature file for offline SecurityCenter plugin updates. The new option can be specified with the –k option (e.g., /opt/lce/daemons/lce_update_plugins.pl –avk) for the files to be retained in /tmp/.
- Added support for fast sorting of column data in the upcoming version 4.7 of SecurityCenter.
- Added an optimization to the query daemon to give higher caching priority to queries from interactive users over those from automated dashboards and reports.
- The rpm –verify command can now be used to determine whether an installation is intact.

Bugs Addressed

- Fixed an issue that could result in corrupt usernames being included in the vulnerability report. This would in turn cause the SecurityCenter import of the data to fail.
- Fixed an issue in which the vulnerability report's user history data could use excessive memory over time.
- Fixed an issue that could cause a plugin error to crash the LCE server.
- Fixed an issue in which assets with no associated events were not displayed in SecurityCenter's asset summary.
- Fixed an issue that could result in the query daemon crashing and restarting periodically.
- Fixed an issue in which client policies could not be displayed on some systems.
- Fixed an issue that could prevent the stats daemon from initializing properly on systems where the number-silos setting had been increased above an earlier value.
- Disabled discovery of hosts from TASL and Stats Daemon events. This previously made it possible to discover a host that appeared in an event such as Nessus-Host_Scan_Start, but did not actually exist.
- When files are moved to the silo archive, LCE now ensures the proper permissions and ownership. Depending on how the silo archive was created, incorrect permissions previously could have caused an error when attempting to query the archive.
- Syntax errors in the rules.conf file will now produce errors in the application log. Previously, such errors could go undetected, causing unexpected behavior from event rules.

Log Correlation Engine Windows Client 4.2.0 Release Notes - 9/26/2013

The Log Correlation Engine Windows Client 4.2.0 is now available. This release contains the following changes:

New features:

- Malware Scanning: The LCE client will scan running processes regularly for malware, similar to Nessus. The following configuration items can be used to tune the scanning, but should not be specified in LCE Client 4.0.1 policies.
- The frequency of the scan can be controlled by adding <malware-scan-frequency> tags to your LCE Client 4.2.0 policy files, where the value is in seconds between scans; for 1 hour scans:

  ```
  <malware-scan-frequency>3600</malware-scan-frequency>
  ```

- Processes may be whitelisted by adding MD5 checksums of the corresponding .exe files to the <whitelist-hashes> tag:

  ```
  <whitelist-hashes> 0e17d427520db98aa72f5c509f015f5e
  1866eda15efde7fc1d4360da92b315e3</whitelist-hashes>
  ```

- Custom malware hashes can also be specified, and will be flagged as malware if they are detected by the LCE client, via the <custom-malware-hashes> tag:

  ```
  <custom-malware-hashes>0e17d427520db98aa72f5c509f015f5e
  1866eda15efde7fc1d4360da92b315e3</custom-malware-hashes>
  ```

Improvements and bug fixes:

- The LCE Client log is now automatically rotated after 75 MB to lce_client.log.previous
- Specifying "all" in an <event-log> tag now also catches the Application-specific event logs, like TaskScheduler
- When available, the FQDN is used when sending CPU usage data, disk usage data, and heartbeats to the LCE server
- Added detection of generic USB devices (in addition to the already-monitored USB volumes)
- Fixed an issue that could cause sporadic disconnections when sending events rapidly

- Fixed an issue that could cause the LCE Client to be unable to write a policy file in the common data directory after a successful installation
- Fixed an issue where, when a USB device without a volume was detected, there was a possibility that the device would be unavailable for a short timeframe

File Names & MD5 Checksums

File	MD5
lce_client-4.2.0-windows_2003_x86.msi	0e379e3a73ca7c626ff4bc2477ed4e53
lce_client-4.2.0-windows_2008_x64.msi	73c530ec7a16503eee108d6782d8fc32
lce_client-4.2.0-windows_2008_x86.msi	b73807d091eb23d727dbe6ad065637b7

Log Correlation Engine 4.2.2 Release Notes - 12/9/2013

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.2.2, significant enhancements to LCE, and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.2 Administration and User Guide.
- The LCE Server Virtual Machine Quick Start Guide explains how to initially configure the LCE server virtual machine.
- Lowering the number-silos setting can impact data storage. If this setting is lowered after data has been collected, LCE will archive or delete silos ranging outside of the specified maximum when rolling to silo 0. In order for data to be archived in this scenario, the silo archiving settings in lce.conf must be enabled.
- LCE version 4.2 is compatible with SecurityCenter version 4.6.2.2 or later. Older versions of SecurityCenter will work with LCE 4.2 without issues, but will not support many of the new

features available in LCE 4.2. Please contact Tenable Support if you have any questions about compatibility issues.

Upgrading from LCE 4.0.x and below

- In order to enable LCE’s reporting features, the report proxy settings must be configured. This can be done by editing the “Discovery Options” section of lce.conf, or running the /opt/lce/tools/lce-post-install.sh script.
- In order for plugins and other updates to be retrieved, LCE 4.2 must first be activated using your provided activation code. This can be done by running the post-install script referenced above.

Upgrading from LCE 3.x

- Beginning with version 4.0 LCE Clients, their configuration files, now called "policies", must be managed centrally with the LCE Client Manager tool when connected to LCE Server 4.0 or later. Existing configuration files may be converted using the LCE Configuration File Converter tool, and imported/assigned with the LCE Client Manager. LCE Clients connected to an LCE Server 3.6 or earlier may continue to use the traditional configuration files.
- The LCE log archive feature has been removed. Existing logs may continue to be searched via the SecurityCenter's "Raw Log Search", but new logs will be searchable via SecurityCenter's "Events" analysis.

File Names & MD5 Checksums

File	MD5
lce-4.2.2-el5.i386.rpm	d61c1f0b6649634e3c5ac31f28c708ef
lce-4.2.2-el5.x86_64.rpm	78c46d7f81d062210b154a3b9f4ab911
lce-4.2.2-el6.i386.rpm	ec7d0b3197a895857fa32aa24c49fb6f
lce-4.2.2-el6.x86_64.rpm	517631bf7e8a41228018aa623e149e9a
LCE-Server-4.2.2-HyperV.zip	f86db222b22c4491cd89850b352f3a1a
LCE-Server-4.2.2-VMware.ova	b63daad3c1c8b6d11a287efffa30fb6f

Application Notes

Bugs Addressed

This is a bug-fix release only.

- Fixed an issue where some queries could hang, impacting query performance
- Fixed an issue where the LCE Client Manager could not appropriately signal the LCE server process of changes to the LCE Client policies or authorizations.
- Added intelligence to fix a partial database entry that could occur during an ungraceful shutdown or disk failure
- Fixed an issue that could cause a failed import of event vulnerabilities into SecurityCenter
- Fixed an issue that could cause invalid data to be used in an LCE alert generated from using the sensor, event1, event2, type, or user macros in rules.conf
- Fixed an issue where the query service would fail to query a portion of the database with a missing index
- Fixed an issue where the query service would fail to return data if multiple filters for the same indexed attribute were specified but one corresponding value did not exist
- Fixed an issue with the statistics engine that could cause it to stop sending events occasionally on a 64-bit host
- Fixed an issue that could cause false client entries to be listed if the LCE server host was scanned
- Added the lsof package as a dependency
- Fixed an issue where the LCE Report Proxy service did not bind to all listed interfaces in lce.conf
- Fixed a memory consumption issue when reloading discovery plugins
- Fixed an issue where the plugin account activation script could fail to parse the response
- Increased the frequency of threatlist downloads

Log Correlation Engine Windows Client 4.2.1 Release Notes - 12/16/2013

The Log Correlation Engine Windows Client 4.2.1 is now available. This release contains the following changes:

New features:

- The LCE Client can now be configured to scan for unknown processes in addition to malware. Unknown processes are not listed in any database of known good or known bad software.
- If configured to scan for malware or unknown processes, the LCE Client will also scan DLLs loaded by processes and report as malware or unknown, if applicable.

Bug Fixes:

- Fixed an issue with the interpretation of the malware analysis, which could result in incorrect log text (antivirus counts and antivirus reporters) when a malware process was identified.

File Names & MD5 Checksums

File	MD5
lce_client-4.2.1-windows_2003_x86.msi	3ea1ac712e04b24e15c33314d9c22ca4
lce_client-4.2.1-windows_2008_x64.msi	3580ad062b1c54fd3ba99b34b8b7998c
lce_client-4.2.1-windows_2008_x86.msi	439d6f913da8d3ae4ad8a791e36db3b5

2012 and Earlier Tenable Log Correlation Engine

Log Correlation Engine 3.0.1 Release Notes

Log Correlation Engine Windows Client 3.6.1 Release Notes

Log Correlation Engine WMI Monitor Agent 3.6.2 Release Notes - 11/21/2012

Log Correlation Engine Unix Client 3.6.2/3.6.3 Release Notes - 11/22/2012, 11/28/2011

Tenable NetFlow Monitor 3.6.2 Release Notes - 12/2/2011

Log Correlation Engine Windows Client 3.6.2 Release Notes - 2/2/2012

Log Correlation Engine Client 4.0.0 Release Notes - 6/27/2012

Log Correlation Engine 4.0.0 Release Notes - 6/27/2012

Tenable Network Monitor 4.0.1 Release Notes - 8/2/2012

Log Correlation Engine 4.0.1 Release Notes - 8/20/2012

Log Correlation Engine Client 4.0.1 for Red Hat Release Notes - 9/12/2012

Log Correlation Engine 3.0.2 Release Notes

- Log Correlation Engine Windows Client 4.0.1 Release Notes - 10/17/2012
- Log Correlation Engine WMI Monitor Agent 4.0.1 Release Notes - 10/23/2012
- Tenable NetFlow Monitor 4.0.1 Release Notes - 11/1/2012
- Log Correlation Engine 4.0.2 Release Notes - 12/13/2012
- Log Correlation Engine 3.2.0 Release Notes
- Log Correlation Engine 3.4.0 Release Notes
- Log Correlation Engine 3.4.1 Release Notes
- Log Correlation Engine 3.4.2 Release Notes
- Log Correlation Engine 3.6.0 Release Notes
- Log Correlation Engine 3.6.1 Release Notes
- Log Correlation Engine Unix Client 3.6.1 Release Notes - 9/27/2012

Log Correlation Engine 3.0.1 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following describes many of the changes that are included in Tenable Log Correlation Engine version 3.0.1, including significant enhancements that have been made, as well as notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

General Notes

As with any application, it is always wise to perform a backup of your Tenable Log Correlation Engine installation before upgrading.

Upgrading from 3.0.0

There are no special upgrade notes for those users running the Log Correlation Engine 3.0.0. The command syntax for an RPM upgrade is as follows:

```
rpm -Uvh %lt;RPM Package File Name>
```

Upgrading from Tenable Log Correlation Engine 2.0.3

- Please note that as part of the upgrade process your existing data files will be modified. As the nature of Tenable Log Correlation Engine is to collect and retain large amounts of data, Tenable cannot create backups of the existing data files as part of the upgrade process since this would run the risk of exhausting available storage. Please be sure to backup your LCE installation, including data files, prior to performing the upgrade process.

- LCE version 3.x is compatible with Security Center version 3.4.2 or greater. The 3.4.2 version of the Security Center will work with LCE 3.x without issues but does not support the new features. Support for the new LCE 3.x features is available in Security Center 3.4.3 or greater. Please contact Tenable Support at support@tenablesecurity.com if you have any questions regarding this.

- To assist with the upgrade process, we have designed and tested all of the v3.0 clients to be compatible with the LCE version 2.0.3 server, and all of the LCE version 2.0.3 clients to be compatible with the LCE version 3.x server. This way, you may choose in what order and manner the components are to be upgraded within your environment.

- Detailed instructions and notes on upgrading are located in the **Upgrading From LCE 2.x** section of the **Log Correlation Engine 3.0 Administration and User Guide**. Please be sure to review this entire section of the documentation before upgrading.

- Previous versions of LCE (2.x) have been installed to the /usr/thunder directory. Beginning with version 3.0.0, LCE installs to the /opt/lce directory. All related file names, services and file text which previously contained "thunder" now accurately reflect "lce".

- Configuration files, data files and log files from your previous installation of LCE will be left in their original locations. All other files will be removed as part of the upgrade process. The configuration and log files are not used by the upgraded application, but are left for the administrator to be used as reference.

- While the upgrade process updates the data files (silos), it does not move them to the new /opt/lce directory structure. You may choose to do this after you have verified that the upgrade process was successful, but it is not required. If you plan to move the LCE data files, please reference the documentation regarding the **database-directory** directive of the /opt/lce/daemons/lce.conf file.

- All release notes for LCE version 3.0.0 are applicable and should be reviewed. These release notes may be found on the **Tenable Customer Support Portal**, in the **Downloads** section, on the **Log Correlation Engine** page.

Application Notes

LCE Server

- An improvement has been made to the user tracking functionality in which the assignment of usernames is attempted when the user: field for a log has no entry, regardless of whether or not the PRM reporting the log is listed in the trusted plugins file.
- For very large silos, the rollover process would appear to make the LCE unreachable. A modification has been made so that this is no longer an issue.
- Redundant messages in the LCE Server administrative log have been suppressed to improve readability.

LCE Clients Unix/Linux

- If the LCE server is not reachable, booting a FreeBSD system with any of the LCE clients installed will no longer cause FreeBSD system startup issues.
- Upon starting the LCE Client, a log entry is now generated which indicates the client is active and reports the version of the client.
- Performing a "service lce_client status" from a Red Hat system on which the LCE Client is running will no longer incorrectly indicate that the client is stopped.

LCE Client Windows

Upon starting the LCE Client, a log entry is now generated which indicates the client is active and reports the version of the client.

Log Correlation Engine Windows Client 3.6.1 Release Notes

The Log Correlation Engine Windows Client 3.6.1 is now available.

Enhancements and highlighted feature areas for this release:

- Added support for LCE server address to be specified with a hostname instead of an IP address
- Added the ability to specify a directory for recursive file integrity monitoring
- Added reporting of new files added to monitored directories
- Support for MSIEXEC Command Line Install "%ServerName" Parameter
- Improved Remote Host Polling [Multi-Threading]

File Names & MD5 Checksums

LCE Windows Client

File	MD5
lce_client-3.6.1-windows_2003_x86.msi	a8bd57558aabdd2ac5afb79a89da4065
lce_client-3.6.1-windows_2008_x64.msi	ddc3dc8f7f3aca13586aaf4ef481fa8a
lce_client-3.6.1-windows_2008_x86.msi	aa55a0fdae4f03f43bbb667358e3bc5e

Log Correlation Engine WMI Monitor Agent 3.6.2 Release Notes - 11/21/2012

The Log Correlation Engine WMI Monitor Agent 3.6.2 is now available.

Enhancements and highlighted feature areas for this release:

- A new utility has been added, wmi_config_credentials, to read a user's wmi_monitor.conf file and create encrypted credentials so that they can remove plaintext credentials (just username and password) from the wmi_monitor.conf file. Run "wmi_config_credentials -h" for further instructions.
- Permissions on temporary data files were tightened for increased security.
- Windows hosts that are configured to be monitored but not up and on the network at the time when the WMI Monitor is started or restarted will now be queried until they are available. Monitoring will then start as usual. Monitoring will also continue if a remote Windows host disappears from the network and then reconnects.

File Names & MD5 Checksums

LCE WMI Monitor

File	MD5
wmi_monitor-3.6.2-es6.x86_64.rpm	6d117fa5b5741fe2d8e0bb2b37527653
wmi_monitor-3.6.2-es5.i386.rpm	e7338dbc7c13367cd3aceab262b23720
wmi_monitor-3.6.2-es5.x86_64.rpm	7c3951ad83f8548b43e7fe9b43fef573
wmi_monitor-3.6.2-es6.i386.rpm	f8283545f72b8f8507fd85b611e1a2ac

Log Correlation Engine Unix Client 3.6.2/3.6.3 Release Notes - 11/22/2012, 11/28/2011

The Log Correlation Engine Unix Client 3.6.2/3.6.3 is now available.

Enhancements and highlighted feature areas for this release:

- Added audit log parsing for all supported platforms except AIX.
- Minor bug fixes

File Names & MD5 Checksums

LCE Client

File	MD5
lce_client-3.6.3-es4.i386.rpm	e9c00be5305f3cd73a3e050e6fff96fd
lce_client-3.6.3-es4.x86_64.rpm	61d16c8b174c5e5a332c895047ea9061
lce_client-3.6.3-es5.i386.rpm	3af1a7c80f99b34a53392624269e4114
lce_client-3.6.3-es5.x86_64.rpm	cb60dc3aab7aef9666a4c8b273e1682f
lce_client-3.6.3-es6.i386.rpm	6a84811e4ab6a198b2a2f74f2aaeb413
lce_client-3.6.3-es6.x86_64.rpm	4f590d3a6fb409fd913fa9ae5c9ac993
lce_client-3.6.2-fc13.i386.rpm	cd8a1c23884d60f1a25bcee4112d6ec7
lce_client-3.6.2-fc13.x86_64.rpm	999e65ecf6d13da1b8a97c880d349e93
lce_client_3.6.2-Debian.i386.deb	267ac65b36409f306b4711d9d537b5ce
lce_client_3.6.2-Debian.x86_64.deb	f207bcdaccdd1db063032136d57109dd
lce_client-3.6.2-AIX.bff	9cfa71f168d05d4e940d68cdc4ca026f
lce_client-3.6.2-dragon-skw.tgz	2de53a5a8bf41488696ce30050ed7c6b
lce_client-3.6.2-freebsd7_i386.tbz	8f47cd5c83f978a781c2671e40718f1b
lce_client-3.6.2-freebsd8_i386.tbz	5b4502ca159e930e8d3cf4dac07a7930
lce_client-3.6.2-SPARC.pkg.tar.gz	c72c5cd365720bd40b75772b502cb690
lce_client_3.6.2-ubuntu10_i386.deb	53f30842055733275e5186750f27012d
lce_client_3.6.2-ubuntu11_i386.deb	bf333a70ad9a6576590b4ffed5f206e8

File	MD5
lce_client_3.6.2-ubuntu11_x86_64.deb	d51796a52ec0dd7802f22b05edd90810
lce_client-3.6.2-osx.pkg.tar.gz	f553b2072b992723b44760e37224311d

Tenable NetFlow Monitor 3.6.2 Release Notes - 12/2/2011

The Tenable NetFlow Monitor 3.6.2 is now available.

Enhancements and highlighted feature areas for this release:

- Added a -h option for the tfmd command line to print command line options to the screen
- Added a debug option to the configuration file to enable sending RAW EVENT and RAW MESSAGE data to the log file
- Minor bug fixes

File Names & MD5 Checksums

Tenable NetFlow Monitor

File	MD5
TenableNetFlowMonitor-3.6.2-es5.i386.rpm	725922eba72e09c16aae7b72cd4ec5ab
TenableNetFlowMonitor-3.6.2-es5.x86_64.rpm	f042ce7908627dfcefa4b0c4499be11e
TenableNetFlowMonitor-3.6.2-es6.i386.rpm	ccadb5464e8ce6d933245efe8527db96
TenableNetFlowMonitor-3.6.2-es6.x86_64.rpm	53a85d00c731d68c31d0360efc3b0463

Log Correlation Engine Windows Client 3.6.2 Release Notes - 2/2/2012

The Log Correlation Engine Windows Client 3.6.2 is now available. This release contains bug fixes and performance enhancements.

File Names & MD5 Checksums

LCE Windows Client

File	MD5
lce_client-3.6.2-windows_2003_x86.msi	03c612a875dc6cdeda007b47934dc339

File	MD5
lce_client-3.6.2-windows_2008_x64.msi	128bd9c0b34bb72817c141955375f275
lce_client-3.6.2-windows_2008_x86.msi	467e64893b32d02878da6ebebbf4d700

Log Correlation Engine Client 4.0.0 Release Notes - 6/27/2012

The following Log Correlation Engine 4.0.0 Clients are now available:

File Names & MD5 Checksums

LCE Client

File	MD5
lce_client-4.0.0-es5.i386.rpm	656c7f19c4a231dabc1af76422377dfb
lce_client-4.0.0-es5.x86_64.rpm	6f3589de73be22f393f14a79ad5920c5
lce_client-4.0.0-es6.i386.rpm	445bca226cb1552d30a22ea7cf7b9fac
lce_client-4.0.0-es6.x86_64.rpm	d36b5084a7b54982858b9548d4c74b73

NetFlow Monitor

File	MD5
TenableNetFlowMonitor-4.0.0-es5.i386.rpm	f9bd813e2a6ee61f31b3dc76a97877eb
TenableNetFlowMonitor-4.0.0-es5.x86_64.rpm	e63303c3f6163386c07356b75a86c481
TenableNetFlowMonitor-4.0.0-es6.i386.rpm	3da8846d075ac8dd55b7865f1949786c
TenableNetFlowMonitor-4.0.0-es6.x86_64.rpm	1bcaad47480cad241eac7b57dbfd5ae3

Network Monitor

File	MD5
TenableNetworkMonitor-4.0.0-es5.i386.rpm	171bc17f91809b86b1b3544c325491b2
TenableNetworkMonitor-4.0.0-es5.x86_64.rpm	1eecb520323a0e35ffc748604365ee87
TenableNetworkMonitor-4.0.0-es6.i386.rpm	ee1c3bb7a249d20ead877e1409bf5ace
TenableNetworkMonitor-4.0.0-es6.x86_64.rpm	07d437da59c246d1e6df5060b291b708

WMI Monitor

File	MD5
wmi_monitor-4.0.0-es5.i386.rpm	b13b6a8452a449fe5339026993dceefa
wmi_monitor-4.0.0-es5.x86_64.rpm	a360cef209741f07614d5172040772d0
wmi_monitor-4.0.0-es6.i386.rpm	3e440bd2c408e47fbffe7398551aa831
wmi_monitor-4.0.0-es6.x86_64.rpm	bca720f6d9b0598d19086c262fb03fdd

Log Correlation Engine 4.0.0 Release Notes - 6/27/2012

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.0, significant enhancements to the LCE, and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- LCE version 4.0 is compatible with SecurityCenter version 4.2 or later. Older versions of Security Center may work with LCE 4.0 without issues, but will not support many of the new features. Please contact Tenable Support if you have any questions about compatibility issues.
- Beginning with version 4.0 LCE Clients, their configuration files, now called “policies”, must be managed centrally when connected to LCE Server 4.0 or later with the LCE Client Manager tool. Existing configuration files may be converted using the LCE Configuration File Converter tool, and imported/assigned with the LCE Client Manager. LCE Clients connected to an LCE Server 3.6 or earlier may continue to use the traditional configuration files.
- The LCE log archive feature has been removed. Existing logs may continue to be searched via the SecurityCenter's "Raw Log Search", but new logs will be searchable via SecurityCenter's "Events" analysis.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.0 Administration and User Guide.

File Names & MD5 Checksums

File	MD5
lce-4.0.0-es5.i386.rpm	f121d55d5d869c583b564ed5d3212584
lce-4.0.0-es5.x86_64.rpm	a46e152cda9ff5becd7e32d30d3acfd9
lce-4.0.0-es6.i386.rpm	25e7b9f48960a26d93aea88f3e4047f3
lce-4.0.0-es6.x86_64.rpm	ac089242b91d547a5bc7a0929cf86dee

Application Notes

LCE Features

- Increased performance resulting from improved multi-processing support.
- Load Balancing accross multiple LCE Servers
- Store all logs in highly compressed log stores instead of flat text raw files.
- Full text search. Added support for full log indexing.
- Option to store and query non-matching (un-normalized) logs in the database.
- TCP syslog (rsyslog) support
- LCE server syslog listen port is now configurable.
- The syslog forward-to port is now configurable and the LCE header optional.
- Centralized Client Configuration Management
- Increased maximum silo size to 10GB per silo
- Enhancements in the client communication:
    - Support for NAT
    - Added event compression between LCE clients and LCE Server
    - Support for multiple secrets covering the same IP range in the server
    - Support higher number of clients

More information about reasons to upgrade to LCE 4.0 may be found at the Tenable website.

Tenable Network Monitor 4.0.1 Release Notes - 8/2/2012

The Tenable Network Monitor 4.0.1 is now available. This release contains the following changes:

- Increased the client robustness when receiving a policy that cannot be used. The client previously revoked policies with parse errors, reverting to the previous operating policy if applicable. Now the client will also revoke policies that parse but have invalid data (for instance an invalid filter-expression).
- Corrected the client usage of statistics-frequency when statistics-frequency is set to 0 or missing. Previously, the client would write statistics as often as possible if the statistics-frequency was omitted from a policy. The client would also continue to write statistics if the policy were updated with statistics-frequency set to 0.

File Names & MD5 Checksums

File	MD5
TenableNetworkMonitor-4.0.1-es5.i386.rpm	d9f301a566ac70382ce5b81c0549563c
TenableNetworkMonitor-4.0.1-es5.x86_64.rpm	88734b6df3f1151c880ad7bc1ff6ee59
TenableNetworkMonitor-4.0.1-es6.i386.rpm	be0c6917fa115eb5d4c02587e6527c1f
TenableNetworkMonitor-4.0.1-es6.x86_64.rpm	0f5a1f76a99da7461e9e9e0052d5e76c

Log Correlation Engine 4.0.1 Release Notes - 8/20/2012

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.0.1, significant enhancements to the LCE, and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.0 Administration and User Guide.
- Lowering the number-silos setting can impact data storage. If this setting is lowered after data has been collected, LCE will archive or delete silos ranging outside of the specified

maximum when rolling to silo 0. In order for data to be archived in this scenario, the silo archiving settings in lce.conf must be enabled.

Upgrading from LCE 3.x

- LCE version 4.0 is compatible with SecurityCenter version 4.2 or later. Older versions of Security Center may work with LCE 4.0 without issues, but will not support many of the new features. Please contact Tenable Support if you have any questions about compatibility issues.
- Beginning with version 4.0 LCE Clients, their configuration files, now called “policies”, must be managed centrally when connected to LCE Server 4.0 or later with the LCE Client Manager tool. Existing configuration files may be converted using the LCE Configuration File Converter tool, and imported/assigned with the LCE Client Manager. LCE Clients connected to an LCE Server 3.6 or earlier may continue to use the traditional configuration files.
- The LCE log archive feature has been removed. Existing logs may continue to be searched via the SecurityCenter's "Raw Log Search", but new logs will be searchable via SecurityCenter's "Events" analysis.

File Names & MD5 Checksums

File	MD5
lce-4.0.1-es5.i386.rpm	bf7bfcd869fc4c7fc6eff5939eafde31
lce-4.0.1-es5.x86_64.rpm	768345e8ea1467a7e9e93c9b0524d615
lce-4.0.1-es6.i386.rpm	0fe4f96c36248bf466be50088e1b15d5
lce-4.0.1-es6.x86_64.rpm	f6eb4964d0e557542f8a78a0508ba84c

Application Notes

New Features/Improvements

- Logs imported using the command line import_logs utility are now automatically indexed, allowing full text searches to be performed on the resulting archives.
- The log importer utility now conforms to the store-unnormalized setting in lce.conf, allowing unnormalized logs to be imported.

- Added Client Manager support for a policy and sensor to be specified prior to authorizing a client.
- Added Client Manager support for configuring a client to operate on the loopback interface.
- Added Client Manager support for hostnames to be specified instead of IP addresses.
- Added support for hostnames in the load balancing configuration options.
- Changes made in the Client Manager now take effect immediately, without the need to exit the utility.
- The SecurityCenter/LCE Manager sensor filter and sensor summary are now case insensitive.
- If the LCE is configured as a load balancing auxiliary server, it will now fail to start and log an error if the primary server is not available when the service is started.
- Added support for an environment in which only a subset of the clients are located behind a NAT.

Bugs Addressed

- Fixed a crash that occurred on 64-bit systems when the server was shutting down. This resulted in a debug file being generated in the log directory upon each service stop or restart.
- Fixed an issue preventing silo .ndb files from being compressed after they became inactive.
- Fixed an issue where the LCE server occasionally forced a client to reconnect.
- Fixed an issue resulting in false positive results for some text searches utilizing the NOT operator.
- Fixed an issue resulting in inaccurate sensor names for some logs.
- Fixed an issue resulting in the server application log flooding with entries after an error on the client communication interface.
- Fixed an issue where new configuration options were not added on upgrade from LCE 3.x when the existing lce.conf file was larger than 32KB.
- Fixed an issue where the query daemon crashed and restarted when a single punctuation character was searched.
- Fixed an issue resulting in event count discrepancies when drilling down into an event type in the SecurityCenter or LCE Manager.

- Fixed an issue where raw.gz files were not deleted after rolling over to a silo that previously contained LCE 3.x data.
- Fixed an issue where LCE 3.x data was no longer searchable from the SecurityCenter or LCE Manager after an upgrade to LCE 4.0.

Log Correlation Engine Client 4.0.1 for Red Hat Release Notes - 9/12/2012

The Log Correlation Engine Client 4.0.1 for Red Hat is now available. This release contains the following changes:

- Resolved an issue where it was possible to get an additional event per log during a policy update.
- Resolved an issue where the removal of statistics-frequency or heartbeat-frequency, or modifying these values in a policy and then updating the policy client-side, could potentially result in an inaccurate reporting frequency of heartbeat log messages or client statistic log messages.
- Resolved an issue where rapid policy changes or modifications server-side could result in the client using an outdated policy.

File Names & MD5 Checksums

File	MD5
lce_client-4.0.1-es5.i386.rpm	d94d357d410efb80f1dcd668c4f125ce
lce_client-4.0.1-es5.x86_64.rpm	c0e02d3863bf6088ade3d3369529c34e
lce_client-4.0.1-es6.i386.rpm	752a8956a0f4826b90fc1c43eb115171
lce_client-4.0.1-es6.x86_64.rpm	3a00a0e330a2334f6bf68acca7541ed2

Log Correlation Engine 3.0.2 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following describes many of the changes that are included in the Log Correlation Engine (LCE) version 3.0.2, including significant enhancements that have been made, as well as notes for upgrading.

Upgrade Notes

- As with any application, it is always wise to perform a backup of your LCE installation before upgrading.
- Please note that as part of the upgrade process your existing data files will be modified. As the nature of LCE is to collect and retain large amounts of data, Tenable cannot create backups of the existing data files as part of the upgrade process since this would run the risk of exhausting available storage. Please be sure to backup your LCE installation, including data files, prior to performing the upgrade process.
- LCE version 3.0.2 is a maintenance release intended to address known issues. It does not have any functional changes from LCE 3.0.0. Please refer to the Release Notes for LCE 3.0.0 for a complete description of LCE 3.0 changes and upgrade recommendations. Please contact Tenable Support if you have any questions regarding this.

Application Notes

The following issues have been resolved in the LCE 3.0.2 update:

- An issue has been addressed that caused the LCE daemon to crash at a silo roll when PRM's are added to the disabled-prms.txt.
- The silo size will now correctly set to 4G (4 gigs) when specified in lce.conf.
- If a PRM specifies only a destination IP, it will not get dragged over to the source IP as well.

Log Correlation Engine Windows Client 4.0.1 Release Notes - 10/17/2012

The Log Correlation Engine Windows Client 4.0.1 is now available. This release contains the following changes:

- Compatible with LCE Server 4.x.
- The LCE Windows Client application now supports the LCE 4.x policy configuration. All configuration of the monitored event logs and monitored files is now done via the LCE 4.x server. Please see the LCE Client Guide for details on creating customized monitoring policies. The LCEConfig application is now obsolete for configuration.
- Text log files being tailed may now be deleted by the LCE Windows Client upon reaching a configurable size, if desired.
- Fixed an issue where adding or removing a PnP device from a machine running the LCE Windows Client could result in a lockup of PnP ports for several minutes.

- Fixed issues concerning stopping the LCE Windows Client service and reconnecting to the LCE Server.

File Names & MD5 Checksums

File	MD5
lce_client-4.0.1-windows_2003_x86.msi	81b0ad1cb2893fd7702cbf4752a974fe
lce_client-4.0.1-windows_2008_x64.msi	4c8556346d41a1e5def408b8a84cff93
lce_client-4.0.1-windows_2008_x86.msi	d364af5f9e192e3163932eb0881d2bdf

Log Correlation Engine WMI Monitor Agent 4.0.1 Release Notes - 10/23/2012

The Log Correlation Engine WMI Monitor Agent 4.0.1 is now available. This release contains the following changes:

- Credentials for hosts that previously had no credentials will be read dynamically while the WMI Monitor is running. After running wmi_config_credentials, there is no need to restart the WMI Monitor.
- Fixed an issue that could result in receiving too many client statistics events if a "statistics-frequency" key was omitted from a client policy.
- Fixed an issue that could result in the client using the wrong policy if multiple rapid changes were made to the client policy server-side.
- Fixed an issue where running wmi_config_credentials from a directory other than the install directory would result in an incorrect detection of the configured remote hosts.

File Names & MD5 Checksums

File	MD5
wmi_monitor-4.0.1-es5.i386.rpm	5e819c6e808692eda83df803dc5af819
wmi_monitor-4.0.1-es5.x86_64.rpm	24d999bf0434f073ad653c4aee8bd185
wmi_monitor-4.0.1-es6.i386.rpm	4cce083b7440b4abbe8bc460f732807c
wmi_monitor-4.0.1-es6.x86_64.rpm	dd9b5477acc35356c9a0ea49d2028c04

Tenable NetFlow Monitor 4.0.1 Release Notes - 11/1/2012

The Tenable NetFlow Monitor 4.0.1 is now available. This release contains the following changes:

- Fixed an issue that could result in receiving too many client statistics events or heartbeats if a "statistics-frequency" or "heartbeat-frequency" key was omitted from a client policy or changed to 0.
- Fixed an issue that could result in the client using the wrong policy if multiple rapid changes were made to the client policy server-side.
- Fixed an issue that could result in the client service shutting down if a policy with an invalid port or protocol was specified in an include-filter or exclude-filter section.

File Names & MD5 Checksums

File	MD5
TenableNetFlowMonitor-4.0.1-es5.i386.rpm	7ccf633093ffec56421c08dbaf307aab
TenableNetFlowMonitor-4.0.1-es5.x86_64.rpm	c0e75e7d84ed874f5303f8d36b9dae20
TenableNetFlowMonitor-4.0.1-es6.i386.rpm	7df8516f69ac91a337690f3da97ab8b8
TenableNetFlowMonitor-4.0.1-es6.x86_64.rpm	d078c0e827395498704af1c57c7cbde8

Log Correlation Engine 4.0.2 Release Notes - 12/13/2012

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 4.0.2, significant enhancements to the LCE, and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 4.0 Administration and User Guide.
- Lowering the number-silos setting can impact data storage. If this setting is lowered after data has been collected, LCE will archive or delete silos ranging outside of the specified maximum when rolling to silo 0. In order for data to be archived in this scenario, the silo archiving settings in lce.conf must be enabled.

Upgrading from LCE 3.x

- LCE version 4.0 is compatible with SecurityCenter version 4.2 or later. Older versions of Security Center may work with LCE 4.0 without issues, but will not support many of the new features. Please contact Tenable Support if you have any questions about compatibility issues.
- Beginning with version 4.0 LCE Clients, their configuration files, now called “policies”, must be managed centrally when connected to LCE Server 4.0 or later with the LCE Client Manager tool. Existing configuration files may be converted using the LCE Configuration File Converter tool, and imported/assigned with the LCE Client Manager. LCE Clients connected to an LCE Server 3.6 or earlier may continue to use the traditional configuration files.
- The LCE log archive feature has been removed. Existing logs may continue to be searched via the SecurityCenter's "Raw Log Search", but new logs will be searchable via SecurityCenter's "Events" analysis.

File Names & MD5 Checksums

File	MD5
lce-4.0.2-es5.i386.rpm	[c367546e70881f580fddba36c041f376]
lce-4.0.2-es5.x86_64.rpm	[3642feb6fbbbd6b5ef21b194115bdf21]
lce-4.0.2-es6.i386.rpm	[ba514baceea2554e2587022db61720b3]
lce-4.0.2-es6.x86_64.rpm	[5e0053465894754cdeb1336169e15b1c]

Application Notes

New Features/Improvements

- The default configuration file has been reorganized into three broad sections, each with several categories of options. On upgraded systems, this file is available as /opt/lce/admin/lce.conf.default.
- A new post-install configuration script has been added. The script runs only on a new install, and provides an interactive walkthrough designed to configure all of the basic settings required for the LCE server to begin collecting logs. This configuration includes the following:

    - The LCE license key
    - The syslog, client-server, and reliable syslog port numbers. The script detects if any of the server's required ports are in use.
    - Network ranges
    - Database directory
    - Syslog sensor names
- LCE now provides the option of defining rules specifying the IP address and port on which each client should connect to the server. This provides added flexibility, such as in configuring firewall operation and determining how network interfaces will be used. Defining rules in NAT environments ensures that clients are assigned the required server address.
- Text searches are applied to tokens in the log, which were previously defined as any sequence of letters, numbers, and dots. For example, searching for "john" in logs containing "john.smith" would not return results, since "john.smith" was a single token. Dots are no longer considered to be part of a token, so searching for "john" or "smith" in the example would now return results. Note that this change will only affect logs stored after the upgrade.
- Automatic plugin updates were previously only performed upon a silo roll. If a silo does not roll for 3 days, the plugins will now be automatically updated as well.
- Event rules can now be defined for internally-generated LCE events, such as client authorization events, full disk alerts, and new TCP syslog connections.
- LCE now generates the LCE-Plugin_Update_Failed event to notify the administrator of failures to update plugins due to errors.

Issues Addressed

- Fixed an issue in which an extraneous, commented-out plugins-directory setting in lce.conf caused an error during plugin updates.
- Fixed an issue in which using the $user variable in an event rule triggering on an internal event caused the server to fail and restart.
- Fixed an issue in which a normalized database file larger than 2GB could not be queried properly.

- Added a 60-second timeout with three retries for plugin updates. This prevents the server from hanging when an invalid proxy is being used for plugin updates.
- Fixed an issue in which the LCE-Agent_Authorization_Granted event was logged for connecting clients that were already authorized.
- Fixed an issue preventing alerts from being generated when the configured disk-alert-percentage was reached. The LCE-High_Disk_Usage event will now be logged when the disk reaches the specified threshold.
- Fixed an issue in which revoking the access of a client using the LCE server's client manager resulted in de-authorizing all clients with the same IP address.

Log Correlation Engine 3.2.0 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe many of the changes that are included in Log Correlation Engine (LCE) version 3.2.0, including significant enhancements that have been made, as well as notes for upgrading. A PDF file of these release notes is also available here.

Note: Additional 3.2 clients will be released separately.

Upgrade Notes

- As with any application, it is always wise to perform a backup of your LCE installation before upgrading.
- LCE version 3.2.0 is compatible with Security Center version 3.4.0 or greater. The 3.4.4 version of the Security Center will work with LCE 3.0 without issues but does not support many of the new features. Support for the new LCE 3.2 features is available in Security Center 3.4.4 or greater. Please contact Tenable Support at support@tenablesecurity.com if you have any questions regarding this.
- To assist with the upgrade process, Tenable has designed and tested all of the version 2.0.x clients and above to be compatible with all of the LCE version 2.0.x servers and above. Because of this, you may choose in what order and manner the components are to be upgraded within your environment.

Thunder to LCE Upgrade Related

- For upgrades from Thunder 2.0.3 to LCE 3.x, configuration files, data files and log files from your previous installation of LCE will be left in their original locations. All other files will be removed as part of the upgrade process. The configuration and log files are not used by the upgraded application, but are left for the administrator to be used as reference.
- While the upgrade process updates the data files (silos), it does not move them to the new /opt/lce/ directory structure. You may choose to do this after you have verified that the upgrade process was successful, but it is not required. If you plan to move the LCE data files, please reference the documentation regarding the database-directory directive of the /opt/lce/daemons/lce.conf file.
- Previous versions of LCE (2.x) installed to the /usr/thunder/ directory by default. Beginning with version 3.0.0, LCE installs to the /opt/lce/ directory by default. All related file names, services and file text that previously contained "thunder" now accurately reflect "lce".
- Please note that for upgrades from Thunder 2.0.3 or earlier, as part of the upgrade process, existing data files will be modified. As the nature of LCE is to collect and retain large amounts of data, Tenable cannot create backups of the existing data files as part of the upgrade process since this would run the risk of exhausting available disk storage. Please be sure to backup your LCE installation, including data files, prior to performing the upgrade process.
- Detailed instructions and notes on upgrading are located in the Upgrading from LCE 2.x section of the Log Correlation Engine 3.2 Administration and User Guide. Please be sure to review this entire section of the documentation before upgrading.

Application Notes

LCE Server Related

- Users now have the Security Center option under "Events" -> "Search Raw Logs" to view historical LCE data across multiple LCEs. Because of the potential for large amounts of LCE data, raw logs are stored compressed on the LCE servers and on the Security Center. This feature requires configuring two options in /opt/lce/daemons/lce.conf: "enable-log-archiving" and "archive-directory". Data collected through "enable-log-archiving" is stored in the directory specified by "archive-directory".
- The TASL engine now performs extensive logging of syntax errors as well as runtime exception conditions. The log file is named tasl_scripts.log, and is stored in the LCE log directory (by default: /opt/lce/admin/log/).

The following new option has been added to lce.conf to accommodate clearing this log:

```
# In addition to the performance report, the TASL processor logs
# detailed technical information related to scripts such as syntax
and
# runtime errors. This data is written to a file called
# tasl_scripts.log in the log directory. Since errors in scripts
cause
# log entries to be generated each time they are encountered, this
log
# can potentially grow large. When set to yes, the following option
# causes the log file to be reset each time the scripts are
# automatically updated. As a result, all log messages will be
relevant
# to the currently installed scripts after an update.
clear-tasl-log-on-update yes
```

- The LCE log archive module maintains usage statistics that are available through the Security Center console under "Events" -> "LCE Archive Status" for users that have enabled "enable-log-archiving" for compressed raw log storage.
- User access is configurable on a "per-LCE" basis for raw log data stored using the "enable-log-archiving" function. Configure this option using the Security Center console through "Users" -> "Manage LCE Access".
- Log archives stored using the "enable-log-archiving" function may be searched from the LCE command-line using the "search_logs" command. The command-line format for a search is:

  ```
  # /opt/lce/search_logs [max results] [start date] [end date]
  [boolean expression]
  ```

- Multiple compressed "enable-log-archiving" logs may be rebuilt into a single text file using a new command-line option "rebuild_logs." The usage of the tool is:

  ```
  # /opt/lce/rebuild_logs [full path to target subdirectory]
  ```

  For example, the following command will create a file with the logs that were compressed under the target directory:

```
# /opt/lce/rebuild_logs /opt/lce/log_archive/2009-02-06/1/ &> feb02-2006-1.txt
```

LCE Client Related

- A Splunk Agent is now available to receive log data from multiple Splunk sources and forward log data on to the LCE server. When configuring the external Splunk server, it is necessary to set sendCookedData=false in outputs.conf.
- TNM TCPDump filters (BPF) are now configurable in tnm.conf using the following expression types:

  ```
  # filter-expression "tcp or icmp or udp port 514";
  ```

  These filters determine the data to be processed by the LCE Network Monitor.
- LCE Unix clients on Red Hat, Mac OS X, FreeBSD, Solaris, Ubuntu and AIX systems may now monitor process binary accounting data via the "accounting-file" option in lce_client.conf. An example entry is shown below:

  ```
  # In addition to plain text files, the LCE client is capable of
  # monitoring process accounting data. The accounting-file keyword
  # is used to specify each file that has been configured to store
  # this data on the host. The binary entry for each executed
  # command is converted to an English log and sent to the LCE
  # server.
  accounting-file /var/account/pact
  ```

  In addition to standard process accounting, the Solaris client has the ability to monitor data collected by the Basic Security Module (BSM) and send equivalent logs back to the LCE server.

Log Correlation Engine 3.4.0 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe many of the changes that are included in Log Correlation Engine (LCE) version 3.4.0, including significant enhancements that have been made, as well as notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- LCE version 3.4.0 is compatible with Security Center version 3.4.4 or later. Older versions of Security Center will work with LCE 3.4 without issues, but will not support many of the new features. Please contact Tenable Support if you have any questions about compatibility issues.
- To assist with the upgrade process, Tenable has designed and tested all version 3.0.x clients and above to be compatible with all LCE version 3.0.x servers and above. This design allows you to choose the order and manner the components are to be upgraded within your environment.
- Detailed instructions and notes on upgrading are located in the **Log Correlation Engine 3.4 Administration and User Guide**.

Application Notes

LCE Server Related

- **IDS Correlation**: LCE 3.4 is now capable of managing IDS events from various sources. This functionality is based on what is currently available in Security Center 3.x. LCE can accept events from IDS devices via Syslog and/or SNMP traps. To differentiate between IDS events and ordinary logs in Security Center queries, a new "event2" field has been added to the LCE database schema. An incoming IDS event will be processed by the LCE plugins, as would happen with ordinary log events. The only difference is that for IDS events, the event2 field will be automatically set to the IDS event signature that was determined from the raw IDS event message unless the matching PRM specifies an overriding event2 value. Unless specified in the PRM, ordinary log events will have an event2 value of "none". Secondary events (event2 values) are summarized through the -lcesplash -splashevent2s showids tool. For example, if the following event is received from a Snort sensor:

  ```
  %lt;158%gt;snort[19997]: [1:8428:9] WEB-MISC SSLv2 openssl get
  shared ciphers overflow attempt
  [Classification: Attempted Administrator Privilege Gain]
  [Priority: 1]: {TCP} 192.0.2.117:49523 -> 192.0.2.6:443
  ```

  a single database entry will be recorded. The "Summary by Event" tool will show a "Snort-TCP_Attempted_Administrator_Privilege_Gain" event, which is the normalized event name specified by the matching PRM.

- **Log importer**: LCE now has the capability to import log data. The typical use case would be where historical logs exist from previous months or years. Another use case would be "semi-real time" where logs need to be batch imported into the LCE.

- **Assigning Syslog Sensor Names**: There is a new configuration option to assign sensor names to syslog sources in the lce.conf file:

  ```
  # For logs received via syslog, a sensor name can be assigned to
  each IP
  # address sending data to LCE. This sensor name will be associated
  with
  # all logs from the designated source, regardless of whether or not
  another
  # sensor name is extracted from the log text.
  syslog-sensors-file /opt/lce/admin/syslog_sensors.txt
  ```

  The file syslog_sensors.txt then lists IP addresses and their names such as:

  ```
  192.168.20.100 CiscoPIX Corporate FW#1
  192.168.20.120 CiscoPIX Corporate FW#2
  192.168.20.130 CiscoPIX Corporate FW#3
  ```

- **Event Alerting**: LCE 3.4 has the ability to send alerts based on rules, defined in /opt/lce/daemons/rules.conf, which detail how the LCE can:

  - send emails to one or more users
  - send Syslog data to one or more servers
  - run a user-defined command

  The rules also have the ability to define filters and be rate limited. Tools provided include:

  1. The msmtp SMTP client located in the /opt/lce/tools/ directory, along with a Tenable-produced default configuration file named msmtp.conf.

2. A syslog tool is provided as the /opt/lce/tools/send_syslog executable. It has the following usage:

   ```
   send_syslog (server address 1) [...] [server address N] -message
   "(message)" [-priority #]
   ```

   For example, the following command will send the specified message to two servers with syslog priority 72:

   ```
   # /opt/lce/tools/send_syslog 127.0.0.1 10.0.0.4 -message "Hello
   World" -priority 72
   ```

   Note: the default priority is 36.

- **LCE Client Activity Logging**: LCE Client activity logging is now supported with a new configuration option in the lce.conf file as follows:

  ```
  # When the following line is uncommented, client activity will be
  logged
  # to the LCE database. This includes connect, disconnect, and failed
  login
  # events.
  log-client-activity
  ```

- **Proxy Support**: Proxy support is now available for plugin updates. The new configuration options appear as follows in the lce.conf file:

  ```
  # The following options configure both the automatic and manual
  update
  # processes to use a web proxy server when downloading files from
  Tenable.
  # When these values are commented out, proxy use is disabled.
  # proxy-address 192.168.10.10
  # proxy-user username
  # proxy-password password
  ```

- **Showids**: The current showids IP filters apply to both the source and destination address of each log. LCE now has the ability to filter by source and destination address separately. showids now supports -mipfile, -sipfile, -dipfile, +port, +sport, and +dport arguments.

- **User Tracking**: Users are now tracked by up to three different IP addresses. The user-ip-change event now indicates when a user is localized at a new IP address.

- **Plugin Test Mode**: A test mode is now available for LCE PRM and TASL scripts that attempt to load all of the PRMs and all of the TASLs to verify that the plugins do not have any errors or compilation issues.

LCE Client Related

- **Note**: A recent Microsoft update, Microsoft .NET Framework 2.0 Service Pack 2 Security Update for Windows Vista Service Pack 2 and Windows Server 2008 Service Pack 2 for x64-based Systems - KB974470, has been found to cause the Windows 2008/Vista LCE client service to stop running. Attempts to restart the service manually do not work. This issue affects systems immediately after the Service Pack update and does not affect LCE client installations that occur after the Microsoft patch. A custom reinstall (detailed below) is required to resolve this issue:
    - Uninstall the LCE Client: At the command prompt window, execute "lce_client.exe /uninstall". Now use "Add/Remove Programs" to uninstall the lce client. The uninstall process will finish despite the service warnings.
    - Install the LCE Client again normally.

- **MD5 File Monitoring**: LCE clients have new options available in the lce_client.conf file to monitor file changes. When a specified file is modified, an alert log indicating the change is sent to Security Center. The determination is made by periodically computing file MD5 checksums and comparing each to the previous result. Options include:
    - Specification of a single file for monitoring
    - Specification of files containing a certain extension in a directory for monitoring
    - Frequency for re-computing the MD5 checksums
    - Monitoring of the lce_client.conf file to determine if a configuration change has occurred

Log Correlation Engine 3.4.1 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 3.4.1, including significant enhancements that have been made, as well as notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- LCE version 3.4.1 is a required upgrade for SecurityCenter 4.
- LCE version 3.4.1 is compatible with Security Center version 3.4.5 or later. Older versions of Security Center may work with LCE 3.4.1 without issues, but will not support many of the new features. Please contact Tenable Support at support@tenablesecurity.com if you have any questions about compatibility issues.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 3.4 Administration and User Guide.

Application Notes

LCE IDS Correlation

- LCE receives vulnerability information and IDS correlation signature updates from SecurityCenter 4 so that it can correlate intrusion detection events with vulnerabilities. Correlation is enabled on a per Repository basis within SecurityCenter 4. To enable, login to SecurityCenter 4 as admin, edit a Repository and select the desired LCE(s) in the .LCE Correlation. field. Both the normalized event name and the originating raw IDS event name are available within the SecurityCenter 4 GUI. When browsing events use the .Target IDS Events. filter to display the Correlated IDS events. A sample screenshot can be viewed here.
- As of 3.4.0, LCE is capable of managing IDS events from various sources. This functionality is based on what was available in Security Center 3.x. LCE can accept events from IDS devices via syslog and/or SNMP traps. To differentiate between IDS events and ordinary logs in Security Center queries, a new "event2" field has been added to the LCE database schema. The LCE supports the following types of IDS sources:

- Snort
- Bro
- RealSecure
- Dragon
- IntruVert
- IntruShield
- NetScreen
- NFR
- Fortinet
- PVS
- LCE
- Cisco
- TippingPoint-Sensor
- TippingPoint-SMS

Log Correlation Engine 3.4.2 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

With the release of LCE 3.4.2, Tenable now offers licenses for 50 silo deployments. Historically, we offered 3 silo and 255 silo licenses for log aggregation and event correlation.

File Names & MD5 Checksums

File	MD5
lce-3.4.2-es3.i386.rpm	e123ba37a916cce646e6d643de31cf8f
lce-3.4.2-es4.i386.rpm	07078100817d3e4bda0bfd940575876c
lce-3.4.2-es4.x86_64.rpm	07d1188c913b6e50e0848c58e86aefc5
lce-3.4.2-es5.i386.rpm	2caf4a0ea2c8eb50e5f1ddf836473ecb

File	MD5
lce-3.4.2-es5.x86_64.rpm	f7f0a6df4568a14b817816cad8d6b2c9

Log Correlation Engine 3.6.0 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 3.6.0, significant enhancements to the LCE and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- **A new license key is required for every LCE instance! Existing customers must contact licenses@tenable.com before upgrading. Only LCE instances need a new license, not SecurityCenter or PVS.**
- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- LCE version 3.6 is required for use with the Asset Summary query in SecurityCenter 4.0.3.
- LCE version 3.6 is compatible with Security Center version 3.4.5 or later. Older versions of Security Center may work with LCE 3.6 without issues, but will not support many of the new features. Please contact Tenable Support if you have any questions about compatibility issues.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 3.6 Administration and User Guide.

File Names & MD5 Checksums

File	MD5
lce-3.6.0-es4.i386.rpm	6dcd3dc013503a175cbcc6fbcb282ea5
lce-3.6.0-es5.i386.rpm	818840575ed2608d0eca71a3454a3972
lce-3.6.0-es5.x86_64.rpm	15a71ced0716096c9565c08747a61bb5

Application Notes

LCE Core Performance

- Query caching daemon to improve the performance of browsing and searching log data. The LCE 3.6.0 query system is a replacement for the LCE showids and showids_db modules. Improvements are achieved through a new architecture that maintains memory state between queries and incorporates more efficient data processing algorithms that decrease query response times. Please note that this new query daemon utilizes approximately 1 GB of memory on a continual basis. For full system requirements, please refer to the LCE Administration and User Guide.
- Improved silo rollover processing and indexing. Indexing now occurs as part of normal log processing instead of during silo rollover. The indexing scheme is also more efficient and stores fewer bytes per entry.
- Replaced the POSIX regular expression API with PCRE to improve performance.
- Asset Summary query efficiency improved ***(requires SC 4.0.3)***
- Relaxed port-based VA/IDS correlation

Log Correlation Engine 3.6.1 Release Notes

The following notes describe the changes that are included in Log Correlation Engine (LCE) version 3.6.1, significant enhancements to the LCE and information about upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- As with any application, it is always advisable to perform a backup of your LCE installation and archived logs before upgrading.
- LCE version 3.6.1 is compatible with SecurityCenter version 3.4.5 or later. Older versions of Security Center may work with LCE 3.6 without issues, but will not support many of the new features. Please contact Tenable Support if you have any questions about compatibility issues.
- Detailed instructions and notes on upgrading are located in the Log Correlation Engine 3.6 Administration and User Guide.

File Names & MD5 Checksums

File	MD5
lce-3.6.1-es4.i386.rpm	d9496cc69b984c7940121aabfabc5cd6
lce-3.6.1-es5.i386.rpm	b30997f52eb153fe75aa083d5fe3a3d4
lce-3.6.1-es5.x86_64.rpm	26f29962f50a2dc419f1dbcd06d593ef
lce-3.6.1-es6.i386.rpm	50d5543c184d114fa3de18da3d894c3e
lce-3.6.1-es6.x86_64.rpm	f805f4a5c35964bbdf9016503b8e1e71

Application Notes

LCE Features

- TASL scripts are now included with LCE by default. Previously they had to be downloaded manually from the Tenable Support Portal after installation.
- Ability to disable TASL scripts individually.
- Hourly statistical data related to logging performance available as LCE events. This includes:
  - Logs/bytes per second
  - Number/percentage of logs matched/unmatched
  - Number of events correlating with vulnerabilities
  - Number/percentage of logs from clients, syslog, and IDS
  - Number of TASL alerts generated
- Threatlist detection plugins now download as daily updates to the LCE.
- Managed Ranges is now determined from the "include/exclude-network" ranges defined in the LCE configuration file instead of CustomerRanges.ip. Please make sure this range matches IP addresses that are considered "internal" from an event perspective. Starting with LCE 3.6.1, this range is used by a number of TASL scripts and the Stats daemon to define inbound/outbound/internal specifications for LCE events. Prior to 3.6.1, these ranges were solely used by the Stats daemon. This is different from the "Directions" filter on the SecurityCenter 4.2 events page, which uses the logged-in user's managed ranges to determine event direction.

- Improved stability by adding the ability to automatically restart the lced or lce_queryd daemon after a serious error. If this occurs, an entry is written to the LCE log (e.g., /opt/lce/admin/log/2011May.log).
- New configuration option to manage the amount of memory allocated to the query daemon.

Fixes

- Log messages exceeding the maximum length (2048 char) are now normalized correctly.
- LCE now correctly filters when the port "!=" operator is in use.
- Correctly resets client status back to "Alive" after "Logged in - Dead" condition when new log data or a heartbeat is received.

Log Correlation Engine Unix Client 3.6.1 Release Notes - 9/27/2012

The Log Correlation Engine Unix Client 3.6.1 is now available.

Enhancements and highlighted feature areas for this release:

- Added support for LCE server address to be specified with a hostname instead of an IP address
- Added CIDR format support in specification of network ranges in the NetFlow Monitor
- Added the ability to specify a directory for recursive file integrity monitoring
- Added reporting of new files added to monitored directories
- Added support for simpler syntax when specifying directories for monitoring

Bug fixes:

- Fixed an issue that sometimes caused a tailed file to be re-sent to the server from the beginning as a result of the file being temporarily moved during log rotation

File Names & MD5 Checksums

LCE Client

File	MD5
lce_client-3.6.1-es4.i386.rpm	bb7ebf9c09af4ae6981e91c84fc6d58a
lce_client-3.6.1-es4.x86_64.rpm	f87c341e36851d48faef33f087908441

File	MD5
lce_client-3.6.1-es5.i386.rpm	a46460de4ef575ee9b01bd8517628646
lce_client-3.6.1-es5.x86_64.rpm	bb649d460199a50ae5b51f99dd1e067d
lce_client-3.6.2-es6.i386.rpm	6e5553a6ca369ab3538526ada572f4bd
lce_client-3.6.2-es6.x86_64.rpm	563027fb8558b3ba227ad51934fbfd5b
lce_client-3.6.1-fedora.i386.rpm	47f5e6fb195161de7a69c8c5cc56c022
lce_client-3.6.1-fedora.x86_64.rpm	4be13d379eca4b73d68a85564a4014c4
lce_client-3.6.1-Debian5.i386.deb	4d1f9e59ad34ea0d15ffc2f82e98a7a3
lce_client-3.6.1-AIX.bff	974cccd159526feb3bfedf95a75ea36a
lce_client-3.6.1-dragon-skw.tgz	4682a83a7f1841b3a82312431d467ebb
lce_client-3.6.1-freebsd7.tbz	58e8bf1579ae967317bca98c8cd099b3
lce_client-3.6.1-freebsd8.tbz	ad85c98d989620769606db84d270b8a9
lce_client-3.6.1-SPARC.pkg.tar.gz	fa52980b6c82985a0f6e47c2e93c337f
lce_client_3.6.1-ubuntu10_i386.deb	2d01666887cad569d7d6d0eff9cafd98
lce_client_3.6.1-ubuntu11_i386.deb	f39eed0f2ed28f8f3fd4b928f0e31bce
lce_client_3.6.1-ubuntu11_x86_64.deb	7d5af83ee55d54c97ac4e8685966d8ec

OPSEC Client

File	MD5
lce_opsec-3.6.1-es4.i386.rpm	1083107b061695277de48aeafe0ab32b
lce_opsec-3.6.1-es5.i386.rpm	1fc101e6ad8fec932593e039e54603ae
lce_opsec-3.6.1-es6.i386.rpm	d8b56a296167a5dff6e8f2044cdc595a

Splunk Client

File	MD5
lce_splunk-3.6.1-es4.i386.rpm	b8776442d868775aca9ffa79d54f07ea
lce_splunk-3.6.1-es4.x86_64.rpm	cc43ef3a74130490bd1c4b50d977c595
lce_splunk-3.6.1-es5.i386.rpm	d6cab3bc39a076f83967cc77e4da9d27
lce_splunk-3.6.1-es5.x86_64.rpm	fe31dc5763c2e600fd0acf04aa77a5df
lce_splunk-3.6.1-es6.i386.rpm	0b3db91f6f5be75adda1b4ab09fdb8e8
lce_splunk-3.6.1-es6.x86_64.rpm	90b54dfcc3f1fd713d38094eb306e4fd

NetFlow Monitor

File	MD5
TenableNetFlowMonitor-3.6.1-es4.i386.rpm	17ff08681f96672768cf1e293759cad9
TenableNetFlowMonitor-3.6.1-es4.x86_64.rpm	fe36bf1f1556743640a883d9d712d06b
TenableNetFlowMonitor-3.6.1-es5.i386.rpm	067dc130e5217557255c5b4704c1059e
TenableNetFlowMonitor-3.6.1-es5.x86_64.rpm	b32c2835bbe81bf94a8c7c622bb1bee3
TenableNetFlowMonitor-3.6.1-es6.i386.rpm	19a8812ffbe9ae4adad64a72c3a3ecb4
TenableNetFlowMonitor-3.6.1-es6.x86_64.rpm	69a4a616abd3776f20329081f95d0873
TenableNetFlowMonitor-3.6.1-freebsd7.tbz	677795dd09aa387e23246570e9f6f6b1
TenableNetFlowMonitor-3.6.1-freebsd8.tbz	220035764aa3ce4b5e4a4b7f3adfc0bb

Network Monitor

File	MD5
TenableNetworkMonitor-3.6.1-es4.i386.rpm	02f586718c6283837d1724956a2ad6cb
TenableNetworkMonitor-3.6.1-es4.x86_64.rpm	5fd3f26c84555e90c9178e10021a3b48
TenableNetworkMonitor-3.6.1-es5.i386.rpm	45a31b349fee063178afd209047861f0
TenableNetworkMonitor-3.6.1-es5.x86_64.rpm	c486aa233ab70c5e25fddb00abd53640

File	MD5
TenableNetworkMonitor-3.6.1-es6.i386.rpm	a5162187eb83e50b45119680745f4d56
TenableNetworkMonitor-3.6.1-es6.x86_64.rpm	9ad8a0f9fa9e073d7b12a259f64bfaf3
TenableNetworkMonitor-3.6.1-freebsd7.tbz	ebe30cf359c531213171bcc93945ad37
TenableNetworkMonitor-3.6.1-freebsd8.tbz	99a125edf704018f85e8ec4ceaaf6ae6

RDEP Monitor

File	MD5
TenableRdepMonitor-3.6.1-es4.i386.rpm	3c2034c56ea35b804461aaa33831b711
TenableRdepMonitor-3.6.1-es4.x86_64.rpm	8c58586aad6476371c5375c319b6ad44
TenableRdepMonitor-3.6.1-es5.i386.rpm	26c6d7d7c899319101e779c870f1579b
TenableRdepMonitor-3.6.1-es5.x86_64.rpm	ae2aea1728cc56efb974a6f264a0c8db
TenableRdepMonitor-3.6.1-es6.i386.rpm	3d1a22ab9a0a529b97fc84f942671d1f
TenableRdepMonitor-3.6.1-es6.x86_64.rpm	5c81a8fd2c1e4e651c18c1d3c9920aa5

SDEE Monitor

File	MD5
sdee_monitor-3.6.1-es4.i386.rpm	d02d1eff2c07aa8915adf4d849b25672
sdee_monitor-3.6.1-es4.x86_64.rpm	5076865869a7229cceef68ee17d0237e
sdee_monitor-3.6.1-es5.i386.rpm	6c8fe2112cec78b00089804af07c2297
sdee_monitor-3.6.1-es5.x86_64.rpm	468d14209fe39b4a43cec2223ed5239b
sdee_monitor-3.6.1-es6.i386.rpm	d0c69211e9a12679a9e9641be2f80bca
sdee_monitor-3.6.1-es6.x86_64.rpm	e32441bc7acb8a15b9cfb17fc072d6e2

Tenable Nessus Release Notes

To view EOL Tenable Nessus release notes, see Tenable EOL Release Notes.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

2022 Tenable Nessus

2021 Tenable Nessus

2020 Tenable Nessus

2019 Tenable Nessus

2018 Tenable Nessus

2017 Tenable Nessus

2016 Tenable Nessus

2015 Tenable Nessus

2014 Tenable Nessus

2013 Tenable Nessus

Tenable Nessus 10.4.2 (2023-01-18)

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Nessus 10.4.2:

- Removed the ability to specify a Java executable path from the Tenable Nessus user interface to prevent undesired changes. Administrators can now specify a Java executable path with a nessuscli command: `nessuscli fix --set path_to_java` (for more information, see Fix Commands).

Bug Fixes

Bug Fix	Defect ID	Applies to

Fixed a network socket state that caused Tenable Nessus processes to stall in certain circumstances.	01481734	All Tenable Nessus versions
Enabled TCP keepalives on certain network connections to shorten Tenable Nessus stall times.	01481734	All Tenable Nessus versions

Security Updates

The following are security updates included in Tenable Nessus 10.4.2:

- Fixed a local privilege escalation vulnerability.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Tenable Vulnerability Management FedRAMP environments support Tenable Nessus scanners versions 10.4.0 and later.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- (Automatic upgrades only) If you upgrade Tenable Nessus to a version later than 10.5.0, the Tenable Nessus will first upgrade to 10.5.0 before it upgrades to the desired version.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to update to the newest version before the GA date automatically, set your Tenable Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.

- If you install Tenable Nessus on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
    - Windows 7 SP1
    - Windows Server 2008 SP2
    - Windows Server 2008 R2 SP1

Tenable Nessus 8.15.8 (2023-01-18)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Nessus 8.15.8:

- Removed the ability to specify a Java executable path from the Tenable Nessus user interface to prevent undesired changes. Administrators can now specify a Java executable path with a nessuscli command: `nessuscli fix --set path_to_java` (for more information, see Fix Commands).
- Fixed an issue that prevented users from using the Tenable migration tool to migrate Nessus 10.4.x licensed scanners to Tenable Vulnerability Management.

Security Updates

The following are security updates included in Tenable Nessus 8.15.8:

- Fixed a local privilege escalation vulnerability.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Tenable Vulnerability Management FedRAMP environments support Tenable Nessus scanners versions 10.4.0 and later.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- (Automatic upgrades only) If you upgrade Tenable Nessus to a version later than 10.5.0, the Tenable Nessus will first upgrade to 10.5.0 before it upgrades to the desired version.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to update to the newest version before the GA date automatically, set your Tenable Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- If you install Tenable Nessus on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Tenable Nessus 10.4.3 (2023-03-07)

Security Updates

The following are security updates included in Tenable Nessus 10.4.3:

- Updated OpenSSL to version 3.0.8.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Tenable Vulnerability Management FedRAMP environments support Tenable Nessus scanners versions 10.4.0 and later.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- (Automatic upgrades only) If you upgrade Tenable Nessus to a version later than 10.5.0, the Tenable Nessus will first upgrade to 10.5.0 before it upgrades to the desired version.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to update to the newest version before the GA date automatically, set your Tenable Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- If you install Tenable Nessus on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Tenable Nessus 8.15.9 (2023-03-07)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Tenable Nessus 8.15.9:

- Updated OpenSSL to version 1.1.1t.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Tenable Vulnerability Management FedRAMP environments support Tenable Nessus scanners versions 10.4.0 and later.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- (Automatic upgrades only) If you upgrade Tenable Nessus to a version later than 10.5.0, the Tenable Nessus will first upgrade to 10.5.0 before it upgrades to the desired version.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to update to the newest version before the GA date automatically, set your Tenable Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- If you install Tenable Nessus on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

2022 Tenable Nessus

Nessus 8.15.3 Release Notes - 2022-02-08

Nessus 8.15.3 Release Notes - 2022-02-08

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following are additional enhancements included in Tenable Nessus 8.15.3:

- Updated Nessus with the latest version of Snappy 1.1 (a compression agent).
- Updated Nessus with the latest version libxml2 2.9.11 (an XML parsing utility).

Security Updates

The following are security updates included in Tenable Nessus 8.15.3:

- Fixed a vulnerability related to local privilege escalation in nessusd.exe v18.12.1.20039 (a debugging tool).
- Updated the Tenable Nessus Expat library to version 2.4.4 to address security vulnerabilities identified in previous Expat versions.

  For more information, see the Tenable Product Security Advisory.
- Secured underscore.js (a Javascript library) against arbitrary code injections.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.15.4 Release Notes - 2022-03-30

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Tenable Nessus 8.15.4:

- OpenSSL was updated to the latest version 1.1.1n.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.15.5 Release Notes - 2022-05-26

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Tenable Nessus 8.15.5:

- Updated libexpac to version 2.4.8 to address several security vulnerabilities.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Tenable Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Tenable Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.15.6 Release Notes - 2022-08-10

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Tenable Nessus 8.15.6:

- Addressed a vulnerability where an audit file could be used to bypass PowerShell and execute commands with elevated privileges on a local scanner.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Tenable Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to update to the newest version before the GA date automatically, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Tenable Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.15.7 Release Notes - 2022-11-09

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Tenable Nessus 8.15.7:

- Updated the following libraries to address several vulnerabilities:
  - Updated `libexpat` to 2.5.0.
  - Updated `libxml2` to 2.10.3.
  - Updated `zlib` to 1.2.13.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Tenable Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to update to the newest version before the GA date automatically, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Tenable Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.1.0 Release Notes - 2022-01-31

New Features

The following are the new features included in Tenable Nessus 10.1.0:

- Improved performance and scalability for Tenable Nessus Manager clustering.
- Tenable Nessus now supports the following operating systems:
  - Oracle Linux 8
  - Windows 11
  - Windows Server 2022
  - Ubuntu 18 for Arm/Graviton2
  - Mac 12 (Monterrey)

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Tenable Nessus 10.1.0:

- Updated reports with a consistent look and feel.
- Renamed the **Vulnerability Operations** report template to **Executive Summary**.
- Updated debug report with a list view for better ease of use.
- Reduced CPU utilization of Tenable Nessus when running on Openshift servers.
- Tenable Nessus now discards the results of a dead target if it becomes unreachable mid-scan when the **stop_scan_on_disconnect** flag is on.
- Updated Tenable Nessus to use the latest version of `snappy 1.1.7` (a compression agent).
- Updated Tenable Nessus to use the latest version of `libxml2 2.9.11` (a XML parsing utility).

Security Updates

The following are security updates included in Tenable Nessus 10.1.0:

- Secured `underscore.js` (a Javascript library) against arbitrary code injections.

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed memory allocation handling to better handle allocation errors encountered in certain plugins.	01255145	All Nessus Versions

Fixed a reporting error where multiple vulnerabilities found on a single host were not counted properly.	01268955	Nessus Pro
Fixed a reporting user interface problem where the PDF report option was not being presented.	01233841	Nessus Pro
Improved the build process to address an Amazon Linux package signing error.	01222403	All Nessus Versions
Fixed a report issue where plugins with risk factor **none** would cause empty results.	01235708	Nessus Pro
Fixed a browser zoom issue where some vulnerability and compliance counts would disappear on the percentage bar.	01226908	Nessus Manager, Nessus Pro
Updated the scan API documentation to provide required integer values for severity levels.	01201809	Nessus Manager
Updated Nessus KB article 000001742 to correctly describe the method by which the engine determines that a target host is unresponsive.	01201809	All Nessus Versions
Fixed manager web server performance by increasing file upload handling efficiency.	01048394	Nessus Manager
Fixed an error where the local scanner database item was inadvertently replaced.	01247157	Nessus Manager

Upgrade Notes

- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.

- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
    - Windows 7 SP1
    - Windows Server 2008 SP2
    - Windows Server 2008 R2 SP1

Nessus 10.1.1 Release Notes - 2022-02-08

Security Updates

The following are security updates included in Tenable Nessus 10.1.1:

- Updated the Tenable Nessus Expat library to version 2.4.4 to address security vulnerabilities identified in previous Expat versions.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.

- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.1.2 Release Notes - 2022-03-30

New Features

The following are the new features included in Tenable Nessus 10.1.2:

- You can now install and access Terrascan, a static code analyzer for Infrastructure as Code, on your Nessus Professional or Essentials instance from the new **Terrascan** page. Terrascan is most commonly used in automated pipelines to identify policy violations before insecure infrastructure is provisioned.

Security Updates

The following are security updates included in Tenable Nessus 10.1.2:

- OpenSSL was updated to the latest version 1.1.1n.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.2.0 Release Notes - 2022-05-26

New Features

The following are the new features included in Tenable Nessus 10.2.0:

- Added a new **Scan Summary** tab that highlights important scan data in Nessus Professional.
- You can now configure update plans for Tenable Agents linked to Nessus Manager.
- BYOL scanners can now add scan targets by Instance ID.
- Added the `aws_scanner` flag to the Nessus AWS integration workflow.

> **Note:** The `aws_scanner` parameter is required for Nessus to perform the auto-discovery of targets and provide those targets to Tenable Vulnerability Management. For more information, see Launch Pre-Authorized Nessus Scanner in the *AWS Integrations User Guide*.

- Added details of plugin execution failures to audit trails.

Changed Functionality and Performance Enhancements

The following enhancements are included in Tenable Nessus 10.2.0:

- Enabled audit signing support for Tenable Agent to provide a secure verification capability for audit scanning files.

  For more information, see the Audit Signing Overview KB article.

- Added more detailed logging for node scans.
- Improved compliance reporting performance by removing redundant data from the scan DB file.
- Extraneous data in compliance descriptions is now disabled by default.
- Added a preference setting that limits the amount of data generated by compliance plugins.

Security Updates

The following are security updates included in Tenable Nessus 10.2.0:

- Updated Zlib to version 1.2.12 to address a medium level vulnerability.
- Updated libexpac to version 2.4.8 to address several security vulnerabilities.
- Removed Nessus version information from unauthenticated API calls.
- Updated jQuery UI to version 1.13.0.

For more information, see the Tenable Product Security Advisory.

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed an issue where custom audit files were not included	01321424	Nessus

in user-to-user data transfers.		Manager
VPR data loading is now postponed until after an upgrade-driven restart.	01346169	Nessus Manager, Nessus Professional
Fixed an issue where a database file was incorrectly deleted due to contention.	01346169	Nessus Manager, Nessus Professional
Fixed an issue where plugins would fail to abort when reaching memory limits in certain environments.	01376928	Nessus Manager, Nessus Professional
Fixed an issue where agent scan durations were exceeding the scan window setting.	01338368	Nessus Manager
Fixed an issue where a User-Defined Nessus Agent scan would incorrectly save as an Advanced Agent scan.	01351178	Nessus Manager
Fixed an issue where the Nessus Manager dashboard would not change when plugin rules are applied.	01264988	Nessus Manager
Fixed an issue where Web App Scanning scan configuration options were not editable.	01311212	Nessus Manager, Nessus Professional
Fixed an issue where exported report sections would be incorrectly colored.	01303175	Nessus Professional
Fixed an issue where the report reference text would overlap the surrounding content.	01318470	Nessus Professional
Fixed an issue where linking a Nessus scanner to Tenable Vulnerability Management would fail when designating group memberships.	01378961	Nessus Scanner

Upgrade Notes

- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version before the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version before the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.3.0 Release Notes - 2022-07-11

New Features

The following are the new features included in Tenable Nessus 10.3.0:

- Added the new Tenable Nessus Expert license and the ability to upgrade to Tenable Nessus Expert from the user interface.
- Added new Terrascan scanning features to Tenable Nessus Expert.

- Integrated Bit Discovery into Tenable Nessus Expert as a new scan template: **Attack Surface Discovery**.

  > **Note:** The attack surface discovery scan currently has a limit of discovering 100,000 child domains and displaying 2,500 domain results in the default results view. You can view all the scan results by applying filters. Tenable is working to extend the maximum child domain amount for customers with larger sets of exposed child domains.

- Updated OpenSSL to support version 3.0.5.
- Updated Tenable Vulnerability Management-linked scanners to support differential plugin updates.
- You can now configure trusted certificate authorities (CAs) for individual scans.

Changed Functionality and Performance Enhancements

The following enhancements are included in Tenable Nessus 10.3.0:

- Updated the Tenable Nessus NASL compiler to stop when it encounters file errors.

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed an issue where ACAS colors would appear incorrectly.	01290503	Nessus Manager, Nessus Professional
Fixed an infinite loop issue related to certain HTTP requests.	01369596	All Tenable Nessus versions
Fixed an RDNS lookup issue that affected some Nessus instances. **Note:** To address this bug, Tenable Nessus was modified to use an asynchronous method of reverse DNS lookup. The asynchronous lookup method is unstable in some newer Linux versions, so Nessus instances installed on Linux	01280566	All Tenable Nessus versions

systems still use the original synchronous lookup method. Most Linux users should use the original synchronous method. However, if the synchronous lookup method causes your scans to stall, you can upgrade to the new asynchronous method by running the following command: `nessuscli fix --set rdns.use_asynchronous_lookup`.		

Upgrade Notes

- If you are upgrading to Nessus Expert from a previous version of Nessus, you must upgrade Nessus to 10.3 prior to performing the Expert upgrade.
- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version before the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version before the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Downgrade Notes

- Once you upgrade to Nessus Expert, you cannot downgrade to Nessus 10.2 using the Expert license. Doing so puts the application in a nonfunctional state.

Nessus 10.3.1 Release Notes - 2022-10-26

Security Updates

The following are security updates included in Tenable Nessus 10.3.1:

- Updated the following libraries to address several vulnerabilities:
  - Updated `datatables` to 1.12.1.
  - Updated `moment.js` to 2.29.4.
  - Updated `libexpat` to 2.4.9.
  - Updated `libxml2` to 2.10.3.
  - Updated `zlib` to 1.2.13.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- If you are upgrading to Nessus Expert from a previous version of Nessus, you must upgrade Nessus to 10.3 prior to performing the Expert upgrade.
- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version before the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.

- If you want to manually update your scanners to the latest version before the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
    - Windows 7 SP1
    - Windows Server 2008 SP2
    - Windows Server 2008 R2 SP1

Downgrade Notes

- Once you upgrade to Nessus Expert, you cannot downgrade to Nessus 10.2 using the Expert license. Doing so puts the application in a nonfunctional state.

Nessus 10.3.2 Release Notes - 2022-11-02

Security Updates

The following are security updates included in Tenable Nessus 10.3.2:

- Updated OpenSSL to 3.0.7 to address two high-severity security vulnerabilities.
- Updated the `libexpat` library to 2.5.0 to address a security vulnerability.

For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- If you are upgrading to Nessus Expert from a previous version of Nessus, you must upgrade Nessus to 10.3 prior to performing the Expert upgrade.
- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version before the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version before the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Downgrade Notes

- Once you upgrade to Nessus Expert, you cannot downgrade to Nessus 10.2 using the Expert license. Doing so puts the application in a nonfunctional state.

Nessus 10.4.0 Release Notes - 2022-10-27

> **Note:** There are known issues with using the Tenable migration tool to migrate Tenable Nessus 10.4.0 licensed scanners to Tenable Vulnerability Management. These issues will be fixed in a future patch or release. In the meantime, Tenable recommends running licensed scanners on version 10.3.1 before using the migration tool to link them to Tenable Vulnerability Management.

> **Note:** Nessus 10.4.0 and later are fully supported within Tenable Vulnerability Management FedRAMP environments.

New Features

The following are the new features included in Tenable Nessus 10.4.0:

- You can now activate new Tenable Nessus Professional and Tenable Nessus Expert trials from within the application when you start Tenable Nessus for the first time.
- Tenable Nessus Expert users can now view Terrascan results and generate reports from the Tenable Nessus Expert user interface.
- You can now log in and perform some operations while Tenable Nessus compiles plugins.
- You can now manage multiple agents at once by using bulk commands from the Tenable Nessus Manager user interface.
- Nessus usernames can now contain parentheses — "(" and ")".
- Nessus now has improved log rotation flexibility.
- Nessus now supports FIPS mode communications.
- Nessus now has improved TLS 1.3 support due to the following additions:
  - The ChaCha20 stream cipher with the Poly1305 message authentication code.
  - The Ed25519 and Ed448 digital signature algorithms.
  - The x25519 and x448 key exchange protocols.

Changed Functionality and Performance Enhancements

The following enhancements are included in Tenable Nessus 10.4.0:

- You can now make copies of scan templates.
- ASM scan efficiency improvements.
- Report queue processing improvements.
- Scan note language improvements.

Security Updates

The following are security updates included in Nessus 10.4.0:

- Updated the following libraries to address several vulnerabilities:
  - Updated `datatables` to 1.12.1.
  - Updated `jquery-ui` to 1.13.2.
  - Updated `less.js` to 4.1.3.
  - Updated `moment.js` to 2.29.4.
  - Updated `select2.js` to 4.0.13.
  - Updated `underscore.js` to 1.13.4.
  - Updated `zlib` to 1.2.13.

  For more information, see the Tenable Product Security Advisory.
- Fixed an input validation issue for some input fields that relied on client-side validation.
- Updated Nessus Manager linking so that linking keys for agents, scanners, and nodes are now different from each other.

Bug Fixes

Bug Fix	Defect ID	Applies to
Improved scan start-up performance for scans with many individually enabled plugins.	01363633	All Tenable Nessus versions
Fixed a bug that deleted the local scanner and caused all agents and agent groups to disappear from the Tenable Nessus Manager user interface.	01420559	All Tenable Nessus versions
Fixed a bug that caused the PDF report to show a black background behind hostnames.	01408918	All Tenable Nessus versions
Fixed an issue that caused missing scan results from child nodes of a Nessus cluster.	01395643	Nessus Manager
Improved overall performance when viewing the agents in a cluster group.	01370959	Nessus Manager

The port scanner can now report more than 1024 open ports, if a user configures it to do so.	01074232	All Tenable Nessus versions
Fixed an issue where scans exported as `.nessus` files were missing an encoding identifier.	01426496	All Tenable Nessus versions
Agent plugin updates on cluster child nodes no longer conflict with plugin delivery to agents.	01424572	Nessus Manager
Fixed an issue where scans would stop during the **Pending** status.	01412489	Nessus Manager
Fixed an issue where CVS reports would not list all hosts, depending on which filters were being used.	01403242	All Tenable Nessus versions
Fixed an issue where **Customized Report** options would not take effect.	01448980	All Tenable Nessus versions
Cleaned up deleted scans initiated by Tenable Security Center.	01445862	Nessus Manager
PDF reports now support Japanese characters.	01406825	All Tenable Nessus versions
Cleaned up scan deletion tracking and ensured that items from respective report directories are deleted.	01445862	Nessus Manager

Upgrade Notes

- Tenable Vulnerability Management FedRAMP environments support Tenable Nessus scanners versions 10.4.0 and later.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM)

located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

- (Automatic upgrades only) If you upgrade Tenable Nessus to a version later than 10.5.0, the Tenable Nessus will first upgrade to 10.5.0 before it upgrades to the desired version.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to update to the newest version before the GA date automatically, set your Tenable Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- If you install Tenable Nessus on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.4.1 Release Notes - 2022-11-02

> **Note:** There are known issues with using the Tenable migration tool to migrate Tenable Nessus 10.4.0 licensed scanners to Tenable Vulnerability Management. These issues will be fixed in a future patch or release. In the meantime, Tenable recommends running licensed scanners on version 10.3.1 before using the migration tool to link them to Tenable Vulnerability Management.

Security Updates

The following are security updates included in Tenable Nessus 10.4.1:

- Updated OpenSSL to 3.0.7 to address two high-severity security vulnerabilities.
- Updated the `libexpat` library to 2.5.0 to address a security vulnerability.

For more information, see the Tenable Product Security Advisory.

Bug Fixes

Bug Fix	Defect ID	Applies to
Increased the Tenable Nessus Manager node update payload size.	01441268	Tenable Nessus Manager

Upgrade Notes

- Tenable Vulnerability Management FedRAMP environments support Tenable Nessus scanners versions 10.4.0 and later.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- (Automatic upgrades only) If you upgrade Tenable Nessus to a version later than 10.5.0, the Tenable Nessus will first upgrade to 10.5.0 before it upgrades to the desired version.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to update to the newest version before the GA date automatically, set your Tenable Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to update your scanners to the latest version before the GA date manually, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- If you install Tenable Nessus on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:

- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Server 2008 R2 SP1

2021 Tenable Nessus

Nessus 8.13.2 Release Notes - 2021-04-05

Nessus 8.14.0 Release Notes - 2021-04-05

Nessus 8.15.0 Release Notes - 2021-06-15

Nessus 8.15.1 Release Notes - 2021-08-10

Nessus 8.15.2 Release Notes - 2021-09-20

Nessus 10.0.0 Release Notes - 2021-11-01

Nessus 10.0.1 Release Notes - 2021-11-17

Nessus 10.0.2 Release Notes - 2021-12-14

Nessus 8.13.2 Release Notes - 2021-04-05

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Nessus 8.13.2:

- OpenSSL was updated to the latest version 1.1.1k. For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.

- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.14.0 Release Notes - 2021-04-05

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Nessus 8.14.0:

CVSSv2 and CVSSv3 Support: Configurable Severity Base

- You can choose whether Nessus calculates the severity of vulnerabilities using CVSSv2 or CVSSv3 scores by configuring your default severity base setting. When you change the default severity base, the change applies to all existing scans that are configured with the default severity base. Future scans also use the default severity base. For more information, see Configure Your Default Severity Base in the *Tenable Nessus User Guide*.

- You can also configure individual scans to use a particular severity base, which overrides the default severity base for those scan results. For more information, see Configure Severity Base for an Individual Scan in the *Tenable Nessus User Guide*.
- By default, new installations of Nessus 8.14 or later use CVSSv3 scores (when available) to calculate severity for vulnerabilities. Preexisting upgraded installations from earlier than 8.14 retain the previous default of CVSSv2 scores.

VPR Support for Nessus

- Vulnerability Priority Rating (VPR), the output of Tenable Predictive Prioritization, is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the current threat landscape. VPR helps organizations improve their remediation efficiency and effectiveness by rating vulnerabilities based on severity level – Critical, High, Medium and Low. For more information, see CVSS Scores vs. VPR in the *Tenable Nessus User Guide*.
- You can now view a new tab for scan results, Top Threats by VPR, which displays the 10 most severe vulnerabilities as determined by their VPR score. For more information, see View VPR Top Threats in the *Tenable Nessus User Guide*.
- VPR is a dynamic score that changes over time to reflect the current threat landscape. However, VPR Top Threats reflect the VPR score for the vulnerability at the time the scan was run. To get updated VPR scores for vulnerabilities in a scan, re-run the scan.
- To ensure VPR data is available for your scans, enable plugin updates.

Top 10 Vulnerabilities Report

- Customers can leverage Nessus Professional reporting capabilities to quickly understand and easily communicate the Top 10 vulnerabilities found in a scan. This helps to identify what vulnerabilities need to be remediated first and eliminates additional work of exporting and manually sending out this information. The report includes:
  - Top 10 Critical Vulnerabilities based on VPR and CVSSv2 or CVSSv3 for that scan.
  - Top 10 High Vulnerabilities based on VPR and CVSSv2 or CVSSv3 for that scan.
  - Most Prevalent Plugins by Number of Hosts by VPR and CVSSv2 or CVSSv3 for that scan.

  For more information, see the Nessus Top 10 Vulnerabilities report details.

Apple M1 Chip Support

- Nessus now can be run as a native application on the Apple M1 chip without the need of running it in compatibility mode.

New plugin release notes

- Tenable releases Nessus plugins multiple times a day. You can access a list of recently updated plugins directly from Nessus.

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 8.14.0:

- The Nessus user interface was updated to use more inclusive language.
- Nessus backups now include concatenated certificate container .pem files.

Security Updates

- OpenSSL was updated to the latest version 1.1.1k. For more information, see the Tenable Product Security Advisory.

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed an issue with Nessus agent clustering where not all agent results were shown correctly in the UI when under heavy load, due to DB lock and network connection issues.	01171932, 01154655, 01151990, 01127708	Tenable Nessus Manager
Fixed an issue where group settings would not get honored when linking agents to a clustered Nessus Manager.	01146420, 01128804	Tenable Nessus Manager
Fixed an issue where agent scans could get aborted if the node it was linked to performed a plugin update while the scan was active.	01110648, 01130429, 01139329	Tenable Nessus Manager
Fixed an issue that, in very rare cases, could cause Nessus to crash on the first day of each month when	00947418	All Tenable Nessus versions

attempting to run scheduled scans.		
Corrected the URL displayed for offline Nessus activation to use HTTPS instead of HTTP.	01157224	Nessus Professional, Managed Scanners
Added UI support for specifying an IPv6 address when configuring a proxy server to link a managed scanner.	01121193	Managed scanners
Corrected the online API documentation for the /api#/resources/scans/configure to note that the "name" field is required.	01124234	All Nessus instances

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.15.0 Release Notes - 2021-06-15

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Nessus 8.15.0:

- This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.
- A vulnerability where after an installation occurs and the user runs a repair on the installation. The repair option, which allows any user to execute the action without admin privileges has been disabled.
- Two third-party libraries (SQLitesqlite)were identified as vulnerable and have been updated.

New Features

The following are the new features included in Nessus 8.15.0:

- Nessus CLI now supports a new command, `nessuscli import-certs`, to add certificates, validate that they are matching, and place them in the correct directory.

  For more information, see Nessuscli in the *Tenable Nessus User Guide*.

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 8.15.0:

- Nessus now uses Npcap as a Windows packet capture library, instead of WinPcap, which was discontinued.

  > **Note:** The upgrade to 8.15.0 installs Npcap but does not remove WinPcap in case your system runs other software dependent on WinPcap. If you manually uninstall WinPcap, Nessus cannot automatically downgrade from 8.15.0 to a prior release. If you remove WinPcap from your system but want to install a version of Nessus earlier than 8.15.0, you must manually install earlier versions via the download package. Similarly, a new installation of Nessus 8.15.0 cannot automatically downgrade to earlier versions; you must manually install earlier versions via a download package.

- The Windows 2008 OS is no longer supported.
- Implemented multiple improvements for logging:
  - A new log file, nessuscli.log, logs all Nessus CLI operations.
  - Improved logging to show successful and failed scan uploads.
  - Improved logging for www_server.log to show start, end, and elapsed times for each access to the Nessus web server.
  - Nessus scanner type added to the log.
  - pre_sig.txt & post_sig.txt have been combined into other_logs.txt.
  - Nessus now uses milliseconds timestamps in backend.log.
  - Added to logs when a scan fails due to missing files instead of ignoring.
  - Advanced settings of **agent scan** for "Audit Trail Verbosity" and "Include the KB", settings override the server **advanced settings** called "agent_merge_audit_trail" and "agent_merge_kb" if disabled to ensure proper function.
- A new Advanced Setting, **merge_plugin_results**, was added to support merging plugin results for plugins that generate multiple findings with the same host, port, and protocol. This setting is recommended to be enabled for scanners linked to Tenable Security Center.

  For more information about the features and functionality supported in this release, see the Nessus 8.15 User Guide.

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed an issue where agents would not link after transitioning from Nessus Manager to Tenable Vulnerability Management.	--	Nessus Manager
Fixed an issue where scheduled scans in Nessus Manager would fail	01194448	Nessus Manager
Fixed an issue where there is a discrepancy in CSV file generated from compliance scan export vs what is shown in the UI	--	All Nessus scanners

Fixed an issue where an IPv6 target scan would fail.	01042585	All Nessus scanners
Fixed an issue where Nessus would ignore certain rules.	00834057	All Nessus scanners

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.15.1 Release Notes - 2021-08-10

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 8.15.1:

- SCE-2799 - Improved scan times by enforcing plugin timeout values. Modified the evaluation order for plugin timeout options to allow for timeout value overrides for all plugins.
- SCE-2828 - Improved plugin compilation speed.

Bug Fixes

Bug Fix	Defect ID	Applies to
Improved scan times by fixing an issue that caused slow plugin behavior after a plugin timeout. (SCE-2829)	01229610, 01237984, 01067282	All Nessus versions
Fixed an issue with memory usage tracking that could cause plugin aborts and Agent connection issues with large Nessus Manager / Agent deployments. (SCE-2832)	01234799, 01233546, 01226819, 01231815, 01232710, 01240941	All Nessus versions

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a

minimum Service Pack to be installed:

- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Server 2008 R2 SP1

Nessus 8.15.2 Release Notes - 2021-09-20

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following additional enhancement is included in Nessus 8.15.2:

- Nessus has been updated with the latest version of OpenSSL 1.1.1l.

  > **Note:** Nessus was not affected by the OpenSSL vulnerability fixed in 1.1.1l. Nessus has only been updated to include the latest version of the OpenSSL library.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.

- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.0.0 Release Notes - 2021-11-01

New Features

The following are the new features included in Nessus 10.0.0:

- Added Nessus 10 support for Raspberry Pi to run scans on the portable, low-cost platform.
- Added Nessus dark mode for easy viewing over long periods of time.
- Added customized reporting in Nessus to tailor reporting data according to your needs.
- Improved plugin compiler for reduced total disk usage, faster initial installation, and faster processing of plugin updates.
- Enhanced user interface experience with list multi-select and scan score details.
- Updated eight existing reports with explanatory descriptions of the represented data.
- Added new Summary tab for agent scan results to provide more-detailed visibility on cluster scans in Nessus Manager.
- Added new Resource Center for announcements, feedback, and Nessus-related help.

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 10.0.0:

- Implemented defragmentation of Nessus databases to reduce transient use of excess disk space during plugin recompilation.
- Added built-in packet capture in Nessus - controllable via scan configuration - to allow for easy debugging of unexpected scan results and network access issues.

- Updated the supported SSL ciphers to remove less-secure CBC ciphers, and updated the default cipher used for Nessus communications for increased security.

Security Updates

The following are security updates included in Nessus 10.0.0:

- Fixed a vulnerability for local privilege escalation in `nessusd.exe v18.12.1.20039` (a debugging tool).

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed an issue where the Nessus Manager file upload API would not return a useful error when called with invalid parameters.	01204820	Nessus Manager
Fixed an issue with enforcement of user access restrictions for agent groups defined with `no access`.	01192413	Nessus Manager
Fixed an issue that would cause the `Credentialed Checks` value on a scan result to wrongly show as `no`.	01265405	All Nessus versions
Fixed the Nessus Manager UI to not show the Plugins tab when viewing the results of an agent scan created from a custom policy.	1168595	Nessus Manager
Fixed an issue that would cause Nessus to crash during scanning on certain OSs by upgrading a third-party library (`libjemalloc`).	01026229, 01156766, 01150178, 01160224	All Nessus versions
Fixed an issue where a requested abort of a Nessus scan would take longer than expected to complete.	01136479	All Nessus versions
Fixed an issue with scan packet captures that would cause incorrect warnings of packets getting truncated in the scan results.	01076654	All Nessus versions

Supported Platforms

- Red Hat Enterprise Linux 5 is no longer supported.

Upgrade Notes

- Due to the dynamic plugin compilation update, Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Nessus 10.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you upgrade to this version of Nessus and downgrade later on, run the following command to ensure support for Internet Explorer: `nessuscli fix --set ssl_cipher_list=compatible`.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.0.1 Release Notes - 2021-11-17

Tenable Nessus 10.0.1 is a patch release that fixes two high-priority issues that were originally planned for Tenable Nessus 10.1.0. It also makes two (or however many improvements) improvements to the dynamic plugin compiler, including a change to improve compilation performance of daily plugin differential updates, and restores the capability to generate basic scan reports from Tenable Security Center managed scanners.

New Features

The following are the new features included in Nessus 10.0.1:

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 10.0.1:

- Restored the capability to generate basic scan reports from Tenable Security Center-managed scanners.
- Made improvements to the dynamic plugin compiler, including a compilation performance improvement for daily plugin differential updates.

Security Updates

The following are security updates included in Nessus 10.0.1:

-

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed a timezone calculation issue with Agent scan scheduling that could cause the scan window to be incorrectly calculated.	01204521	Tenable Nessus Manager
Fixed an issue specific to Tenable Agent clustering environments in which the `track_unique_agents` preference was being ignored.	01245814	Tenable Nessus Manager

Supported Platforms

-

Upgrade Notes

- Due to the dynamic plugin compilation update, Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Nessus 10.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 10.0.2 Release Notes - 2021-12-14

New Features

The following are the new features included in Nessus 10.0.2:

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 10.0.2:

- To facilitate a rapid response to new and critical security threats, Tenable Vulnerability Management users can now trigger an immediate plugin update on their scanners from the Tenable Vulnerability Management user interface, rather than waiting for the standard 24-hour plugin update cycle.

Security Updates

The following are security updates included in Nessus 10.0.2:

Bug Fixes

Bug Fix	Defect ID	Applies to

Supported Platforms

-

Upgrade Notes

- Due to the dynamic plugin compilation update, Tenable Nessus customers who have custom plugins could experience compilation failures if their plugins do not adhere to the updated standards outlined in the NASL Library Optimization guide. We recommend that customers with custom plugins review this guide and make any necessary updates before updating to Tenable Nessus 10.0.x.
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Tenable Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you want your scanners to automatically update to the newest version prior to the GA date, set your Nessus Update Plan to **Opt in to Early Access releases**.
- If you want to manually update your scanners to the latest version prior to the GA date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:

- Windows 7 SP1
- Windows Server 2008 SP2
- Windows Server 2008 R2 SP1

2020 Tenable Nessus

Nessus 8.10.0 Release Notes - 2020-03-24

Nessus 8.10.1 Release Notes - 2020-05-19

Nessus 8.11.0 Release Notes - 2020-07-14

Nessus 8.11.1 Release Notes - 2020-08-20

Nessus 8.12.0 Release Notes - 2020-10-08

Nessus 8.12.1 Release Notes - 2020-10-29

Nessus 8.13.0 Release Notes - 2020-12-07

Nessus 8.13.1 Release Notes - 2020-12-16

Nessus 8.9.0 Release Notes - 2020-01-23

Nessus 8.9.1 Release Notes - 2020-03-04

Nessus 8.10.0 Release Notes - 2020-03-24

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Nessus 8.10.0:

- **Backup and Restore Tool** - Ability to create Nessus backups that can easily and quickly be restored.

  For more information, see Back Up Nessus and Restore Nessus in the *Nessus User Guide*.

- **Nessus Upgrade Plan** - In Nessus Professional and managed scanners linked to Tenable Vulnerability Management, users can set a Nessus Update Plan that determines the version that Nessus updates to.

  The options are as follows:

  - Update to the latest GA release: Update to the latest version as soon as it is made generally available (GA).
  - Opt in to Early Access releases: Update to the latest version as soon as it is released for Early Access (EA), typically a few weeks before general availability.
  - Delay updates, staying on an older release: Remain on an earlier version of Nessus set by Tenable, which is at least one release older than the current generally available version. When Nessus releases a new version, your instance updates software versions, but stays on a version prior to the latest release. Note: Nessus never updates to a version earlier than 8.10.0, so this setting will impact upgrade to releases after 8.10.0.

  For more information, see Update Nessus Software in the *Nessus User Guide*.

- **Downgrade Option** - Support downgrade to a prior version of Nessus.

  > **Note:** Users cannot downgrade to versions prior to 8.10.0.

  For more information, see Downgrade Nessus Software in the Nessus User Guide.

- **Slow Rollout** - Roll out new Nessus releases to the Tenable Update Server for licensed Nessus Professional and Nessus Manager installations separately from Tenable Vulnerability Management. New Nessus versions will be made GA for Tenable Vulnerability Management-linked scanners to auto-update one week after the GA for the release. The new version will be available on the Tenable Nessus Download page on the GA date, for customers that want to update earlier.

- **Predefine Nessus Manager linking key** - In Nessus Manager, you can manually set the linking key for Agents and Nessus scanners to help streamline deployments.

  For more information, see Retrieve the Linking Key in the *Nessus User Guide*.

- **Specify scanner groups when linking scanners to Tenable Vulnerability Management** - When linking Nessus scanners to Tenable Vulnerability Management using the CLI, you can set the scanner group to which to automatically add the scanner.

For more information, see Nessus CLI in the *Nessus User Guide*.

Changed Functionality and Performance Enhancements

- Quality and stability improvements.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue with Apple IOS MDM Compliance Checks that users were prompted to specify multiple credential types	00934506
Fixed an issue were plugin 10716 caused the scanner to crash	00913088
Fixed issues where high CPU usage was seen during a scan:	
High CPU was seen on scan of Linux Server after upgrade to 8.7.2	00903233
Scans aborting in Tenable Vulnerability Management because nessusd process throttles at 99%	00950793
Fixed issues related to scans running longer than normal or not completing:	
Nessus scans stuck stopping on scanners from Tenable Security Center	00964502
Unofficial External PCI scan never completes	00951214
Tenable Vulnerability Management scan using local scanners is taking days rather than hours	00910893
Tenable Vulnerability Management scan has been "Running" for over 5 days in UI	00903231
External PCI Scan taking a lot longer than usual	00918023
Scan taking longer than it should	00901325
Scans inconsistently ending in 'partial' status due to scanners timing out	00852594
Scans failing to complete	00815880

Upgrade Notes

- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus 8.10.1 Release Notes - 2020-05-19

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: Nessus 8.10.1 for the AWS Graviton2 platform is available as an Early Access release. Try it here: https://www.tenable.com/downloads/nessus-early-access

New Features

The following are the new features included in Nessus 8.10.1:

- **Added Option to Force Stop a Scan Job** - Added the ability to force a scan job to stop.

  For more information, see Stop a Running Scan in the *Nessus User Guide*.

Changed Functionality and Performance Enhancements

- **Increased time window for marking an agent as offline** - Improved the determination of when an agent should be considered offline.
- **Upgraded Nessus to use OpenSSL 1.1.1g.**
- **Streamlined application of large cloud-based exclusion lists to improve scan performance.**

Bug Fixes

Bug Fix	Defect ID
Fixed an issue with target scanning access not being enforced consistently for Tenable Vulnerability Management scans.	00921904
When a recast rule is used for an emailed report the recast rule was ignored.	00924963
Resolved an issue where scans run on the first of the month filled-up the disk space with verbose log detail for certain customers.	00947418
When using the "CVSS Vector Contains" filter in Nessus Pro, results did not match the filter.	00970121
Email notification for agent scans did not send when clustering is enabled.	00975051
For Agent scans in clustered environment, the "plugin_set" value was not available in .nessus exports.	00979699
Resolved issue when processing large exclusion lists that caused delays in starting scans.	00984830
Exported HTML/PDF did not display enumerated service names.	00998344
Agent scan in clustered environment was reporting in pending state rather than running.	01003033
Improved the determination of when an Agent should be considered offline.	00935155
Fixed an issue where Agent blackout windows were not enforced for Agents in a clustering configuration.	-

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.11.0 Release Notes - 2020-07-14

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

- Improved the performance of scans configured with large Tenable Vulnerability Management exclusion lists.
- Nessus builds are now significantly smaller (around half the size) due to the removal of deprecated audit content.
- Added log rotation for the nessusd.dump log file, including user-configurable settings to control rotation. See Advanced Settings and Manage Logs in the *Nessus 8.11.x User Guide*.
- Password credentials are now hashed using PBKDF with SHA512 and a 512-bit key length.
- Allow silent installation and uninstallation of Nessus on Windows, for easier automation.

- The advanced settings `ssl_mode` and `ssl_cipher_list` are now enforced for communication from Nessus scanners to other systems. Previously, these settings were only used for inbound connections. This does not impact scanning behavior.

For more information about the features and functionality supported in this release, see the Nessus 8.11.x User Guide.

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed an issue where the scanner setting `multi_scan_same_host` was not being honored consistently.	00998706	All Nessus versions
Fixed a memory leak with encoding conversions that could cause scanners to abort.	01022081	All Nessus versions
Improved the processing of scan policies with large numbers of disabled plugins to prevent timeouts during scan initialization.	00966532	Tenable Vulnerability Management-linked scanners
Fixed an issue where Tenable Vulnerability Management exclusion lists were not being honored if the request to Tenable Vulnerability Management timed out.	01029956	Tenable Vulnerability Management-linked scanners
Fixed an issue with migrating scan policy data to Tenable Vulnerability Management with "audit trail verbosity" setting not recognized by Tenable Vulnerability Management.	01000615	Tenable Vulnerability Management-linked scanners
Added the ability for the parent node in a Nessus Manager cluster to reload running scans after restarting, to prevent scan aborts on plugin updates or other restarts.	01016242	Nessus Manager
Fixed an issue with the list of plugins that appear when creating a scan with a user-defined policy.	00990367	Nessus Professional

Fixed an XSS vulnerability in the Nessus user interface.	-	Nessus Professional

Upgrade Notes

- Due to the removal of some deprecated content, this version of Nessus is noticeably smaller than earlier versions.
- A fix has been made to correctly use the default setting for "multi_scan_same_host", which prevents multiple hostnames that coalesce to a single IP from being scanned in parallel. While this enforces the expected behavior, it may have the effect of slowing down scans in some cases. Customers can change this default behavior on their on-premise scanners by setting "multi_scan_same_host" to "yes".
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.11.1 Release Notes - 2020-08-20

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

- **nessusd.dump Log File Millisecond Timestamps** - When the advanced setting `logfile_msec` is enabled, millisecond resolution is enabled for `nessusd.dump` log file timestamps. Previously, only the `nessusd.messages` log file supported this setting.

  For more information, see Advanced Settings in the *Nessus User Guide*.
- **Added Context for Security Notes** - Nessus scan security notes now show the IP address and plugin ID of the target and plugin that produced the note, adding critical context which is useful for debugging.
- **Duplicate Agent Detection** - Nessus Manager detects duplicates agents that have the same MAC address. When the agent setting `detect_duplicates` is enabled, agents detected as a duplicate automatically unlink and reset its Tenable UUID.
- **Updated jQuery third party library** - Upgraded the version of jQuery used in the online Nessus API documentation, to remove security vulnerabilities reported in the older version.

For more information about the features and functionality supported in this release, see the Nessus 8.11.x User Guide.

Bug Fixes

Bug Fix	Defect ID	Applies to
Added protections to prevent out-of-bounds memory access in the NASL process space.	-	All Nessus versions
Added validation checks to the JSON config file used for streamlined scanner deployment.	01027462	All Nessus versions
Fixed an issue causing the session timeout to not be honored when the user was on the Settings > About page.	-	Nessus Professional, Nessus Manager
Added systemd support for Debian/Ubuntu on	00847209	Nessus

versions that use systemd over init.d, to address an issue with running as non-root user.		Professional
Fixed an issue encountered in Google Chrome where the navigation links were only clickable from the bottom.	00920107	Nessus Professional
Fixed a pagination issue with host discovery scan results when a large number of hosts was returned.	01025309	Nessus Professional
Fixed an issue where Agent scans configured with a 24-hour scan window would miss the next day's launch due to unfinished processing for the current scan.	01020512	Nessus Manager
Updated DB access settings to prevent the possibility of DB corruption on Nessus Manager configured as a Cluster Manager.	01041759	Nessus Manager
Fixed an issue where scanners managed by Tenable Vulnerability Management would not update plugins if a core software update was also pending.	00908570	Tenable Vulnerability Management-linked scanners
Fixed a race condition that could cause scan results to not be detected as completed, resulting in aborted scan chunks.	01025683	Tenable Vulnerability Management-linked scanners

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.12.0 Release Notes - 2020-10-08

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

> **Note:** Tenable recommends upgrading to the patch for this release, Nessus 8.12.1, which includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

New Features

The following are the new features included in Nessus 8.12.0:

- **Agent Cluster Groups**: Tenable Security Center customers using agent clustering now have the ability to organize their cluster nodes and agents into logical cluster groups. This allows customers to configure their agents in a way that conforms to their network topology, ensuring that agents can be assigned to a cluster group that is reachable from their network.

  > **Note:** If cluster child nodes have automatic software updates disabled, you must manually update them to Nessus 8.12 or later to use agent cluster groups. If cluster child nodes have automatic

> software updates enabled, nodes can take up to 24 hours to update. To ensure correct linking and configuration, wait for all child nodes to update to a supported Nessus version before configuring custom cluster groups. All child nodes must be on the same Nessus version and operating system.

For more information, see Cluster Groups in the *Tenable Nessus User Guide*.

- **Predefined Reports for Nessus Professional**: Added three new predefined reports for Nessus Professional customers, allowing users to create HTML or PDF reports that preconfigure the most useful summaries for vulnerability management. Users can create:
  - An Unsupported Software report to provide insight into unsupported software found in the customer's environment.
  - An Exploitable Vulnerabilities report which details all detected vulnerabilities which have known exploits.
  - An OS Detections report which gives lists all operating systems found on the scanned targets.

  For more information, see Create a Scan Report in the *Tenable Nessus User Guide*.
- Support for running Nessus on additional operating systems, including SUSE Linux Enterprise Server 15, FreeBSD 12.x, Kali 2018, 2019, 2020, and Ubuntu 20.04.

  For more information, see Software Requirements in the *Tenable Nessus User Guide*.

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 8.12.0:

- Added additional data to the Nessus debug report, to better assist in troubleshooting, including public/non-secret certificate information and license type and features.
- Removed the **Scanner** tab from the Nessus user interface for all license types except for Nessus Manager.
- In Nessus Manager, linked agents and scanners are now accessed from the new **Sensors** page in the top navigation bar.
- You cannot access a cluster child node via the user interface. Manage agents from the parent node instead.

Bug Fixes

Bug Fix	Defect ID	Applies to
Fixed an issue with using the "pkg add" command for installation on FreeBSD v11	00847180, 00738521	All Nessus versions
Fixed an issue with connections being dropped if Nessus tried to open more than the configured maximum number of concurrent TCP sessions per host for a target	00809878	All Nessus versions
Fixed an issue where the "last scanned" timestamp for an Agent was updated even if the Agent did not report results	01049609	Nessus Manager
Fixed an issue where unlinked Agents were sometimes not being deleted from Nessus Manager	01048912	Nessus Manager
Improved performance of some database queries that were potentially causing Agent merges to fail due to database lock timeouts.	01026793	Nessus Manager
Fixed a bug with target list enumeration that in rare cases was causing Tenable Vulnerability Management cloud scanners to get in an infinite loop and run out of memory	01038386	Tenable Vulnerability Management cloud scanners

Upgrade Notes

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked scanners communicate with.

    - Starting with Nessus version 8.12.0, Tenable Vulnerability Management-linked scanners communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case the sensors are not able to connect to the new domain, they fall back to using cloud.tenable.com. Nessus scanners with earlier versions will continue to use the cloud.tenable.com domain.

    - **Recommended Action** - If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, thus reducing operational overhead. Please contact your Network Administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.

- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.

    - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.

    - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.

- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:

    - Windows 7 SP1

    - Windows Server 2008 SP2

    - Windows Server 2008 R2 SP1

Nessus 8.12.1 Release Notes - 2020-10-29

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.13.0 Release Notes - 2020-12-07

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Nessus 8.13.0:

- **Ability to deploy Nessus as a Docker image for a container** – Users can now access an official Docker image for Nessus to deploy as a container. You can run Nessus offline or online, and the deployment includes plugin support.

For more information, see Deploy Nessus as a Docker Image in the *Tenable Nessus User Guide*.

- **Additional operating system support** – Nessus is now supported on Amazon Linux 2 and Apple macOS Big Sur (11).
- **Agent Remote Configuration** – You can configure some agent settings remotely from Nessus Manager, rather than having to configure the setting directly on the agent.

  For more information, see Modify Remote Agent Settings in the *Tenable Nessus User Guide*.
- **New Predefined Reports for Nessus Professional**– Added three new predefined reports for Nessus Professional customers, allowing users to create HTML or PDF reports that preconfigure the most useful summaries for vulnerability management.

  Users can create:

  - A report summarizing a list of IPs with what vulnerabilities were found in the scan.
  - A report summarizing all known/default accounts found on systems during the scan.
  - A report for vulnerabilities older than one year, which gives insight on when the vulnerabilities were initially reported to be exploitable.

  For more information, see Create a Scan Report in the *Tenable Nessus User Guide*.

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 8.13.0:

- Nessus updated to use OpenSSL 1.1.1h.
- Updated the Nessus user interface to use jQuery v3.5.1, to address a vendor-reported cross-site scripting vulnerability. For more information, see the Tenable Product Security Advisory.
- Prevented downgrading to prior versions if a master password is configured in order to prevent the DB from getting into a corrupted state.
- Increased the default time before Agents are required to relink in Tenable Agent clustering configurations if the parent node is down or unreachable.

- Added capability for Nessus cluster child nodes to link to the Nessus Manager parent node through a proxy.
- Added in-report data descriptions for Nessus Professional pre-defined reports, as well as visual markings to identify Live Results.
- Updated build artifacts to create a separate build for Amazon Linux 2.

Bug Fixes

Bug Fix	Defect ID	Applies to
Updated Nessus to use the same username validation for all user creation methods, including mkcert-client	01081253	All Tenable Nessus versions
Fixed an issue that could cause filtered compliance scan results to not export correctly	01078705	All Tenable Nessus versions
Fixed an issue that could cause Nessus Manager with clustering enabled to create very large, fragmented DB files	01101123	Tenable Nessus Manager
Fixed a potential issue with viewing Agent scan results in Nessus Manager for Agents with multiple NICs configured	01081048	Tenable Nessus Manager
Fixed a condition that was causing a benign but misleading error log message for Tenable Vulnerability Management linked scanners	01075254	Tenable Vulnerability Management cloud scanners
Added cleanup of orphaned scan policy files on Nessus scanners generated from Tenable Security Center launched scans	01064111	Managed scanners
Added a setting to allow global disabling of gzip compression for any responses from the Nessus web server.	N/A	All Tenable Nessus versions

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.13.1 Release Notes - 2020-12-16

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following additional enhancements are included in Nessus 8.13.1:

- Nessus now leverages OpenSSL version 1.1.1i.

Bug Fixes

Bug Fix	Defect ID	Applies to

Fix issue on Tenable Nessus Manager cluster parent node with processing Agent scan results greater than 2GB.	01127708	Tenable Nessus Manager

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- Tenable Vulnerability Management-linked scanners receive the latest software update starting one week *after* the Nessus general availability (GA) date.
  - If you want your scanners to automatically update to the newest version prior to that date, set your Nessus Update Plan to **Opt in to Early Access releases**.
  - If you want to manually update your scanners to the latest version prior to that date, disable automatic updates so the scanner does not automatically downgrade to the previous version.
- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

Nessus 8.9.0 Release Notes - 2020-01-23

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Nessus 8.9.0:

- **Streamlined Sensor Deployment** - Capability to include environmental configuration variables as part of a sensor installation.

  For more information, see Mass Deployment Support in the *Nessus User Guide*.

Changed Functionality and Performance Enhancements

The following are changes to functionality included in Nessus 8.9.0:

- **Open SSL v1.1.1 Update** - Nessus scanners will leverage OpenSSL v1.1.1 as part of this release.

  This causes impact to the ciphers and SSL versions supported. For more information, see the knowledge base article.

- **Capability for Nessus to support plugin databases greater than 4 GB.**

  This causes an automatic full recompilation of the plugins upon first startup after upgrade, which may take several minutes.

Bug Fixes

Bug Fix	Defect ID
Fixed issue where a user was unable to login to Nessus using a certificate	00862610
Fixed issue where remediation tab was not being displayed	00874773
Fixed issue where a basic user could not view results in Nessus Manager	00896771
Fixed issue where a scan with a policy with mixed plugin families would not run	00883290
Fixed issue related to upgrading on Windows platforms from earlier versions of Nessus	00899337
Fixed issue with cloud scans aborting	00911689

Upgrade Notes

- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.9.1 Release Notes - 2020-03-04

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Nessus 8.9.1:

- **Additional SSL cipher options** - Additional security by updating our SSL cipher options to take full advantage of OpenSSL 1.1.1.
- **Additional OS support** - Added support for MacOS Catalina (10.15).

Changed Functionality and Performance Enhancements

The following are changes to functionality included in Nessus 8.9.1:

- Quality and stability improvements.

Bug Fixes

Bug Fix	Defect ID
Fixed issue where a user errantly receives a SIGABRT when running a large scan.	00830386
Fixed issue where SYN Scanner improperly listed ports by first numeral instead of entire port number.	00859512
Fixed issue with Scan config defaulting to UTC instead of system timezone.	00891818
Fixed issue with settings page not loading after upgrade.	00901440
Fixed issue related to poor performance of external PCI scans on AP cloud scanners.	00900847
Fixed issue with Dashboard Tab not showing despite being selected in the scan configuration.	00916022
Fixed issue related to data filtering of agents.	00926282
Fixed issue related to timezone misconfiguration allowing customers to schedule scans in the past.	00922826
Fixed issue with not being able to set the agent blackout window using IE 11.	00944123

Upgrade Notes

- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:
  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1
- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

2019 Tenable Nessus

Nessus 6.12.0 Release Notes - 2019-03-21

Nessus 6.12.1 Release Notes - 2019-08-15

Nessus 8.1.2 Release Notes - 1/9/2019

Nessus 8.2.0 Release Notes - 1/22/2019

Nessus 8.2.1 Release Notes - 1/24/2019

Nessus 8.2.2 Release Notes - 1/31/2019

Nessus 8.2.3 Release Notes - 2/17/2019

Nessus 8.3.0 Release Notes - 2019-03-26

Nessus 8.3.1 Release Notes - 2019-03-29

Nessus 8.3.2 Release Notes - 2019-04-30

Nessus 8.4.0 Release Notes - 2019-05-14

Nessus 8.5.0 Release Notes - 2019-06-25

Nessus 8.5.1 Release Notes - 2019-07-02

Nessus 8.5.2 Release Notes - 2019-08-05

Nessus 8.6.0 Release Notes - 2019-08-13

Nessus 8.7.0 Release Notes - 2019-09-24

Nessus 8.7.1 Release Notes - 2019-09-26

Nessus 8.7.2 Release Notes - 2019-10-10

Nessus 8.8.0 Release Notes - 2019-11-05

Nessus 6.12.0 Release Notes - 2019-03-21

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- **Double the supported size of the Nessus Plugins Database** - The Nessus Engine was updated to support the handling of compiled plugin DBs that exceed 2 GB in size. This prevents newer versions of the Nessus plugins that exceed the 2 GB size from resulting in a failure that would leave the scanner inoperable.

Bug Fixes

- Updated openSSL patch level 1.0.2r to ensure latest security fixes are available

Upgrade Notes

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 6.12.1 Release Notes - 2019-08-15

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue with plugin size causing a significant impact on feed updates and scanning on Nessus Scanners.	N/A
Updated openSSL patch level 1.0.2s.	N/A

Nessus 8.1.2 Release Notes - 1/9/2019

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.1.2.

Bug Fixes

- Fixed an issue with Nessus Scanners running on Linux that could cause them to lock up after a period of scanning.

Nessus 8.2.0 Release Notes - 1/22/2019

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.2.0.

New Features

The following are the new features included in the Nessus 8.2.0 Release:

- **Scanner Health Page:** We recently completed our 4th annual Tenable INIT conference, where each year teams assemble for creative problem solving and a bit of fun. This new capability is a direct output of that event. The Scanner Health page is the first step to providing users scanner information, including real-time insight into health and performance data on a local scanner.

  Examples of details a user can view include host stats; memory and CPU usage as well as application-specific stats including the number of scans running and the number of assets being scanned.

- **Nessus Pro/Manager to Tenable Vulnerability Management Migration:** For some users, there may come a time when they want to move to the Tenable Vulnerability Management platform. For those users, we have now automated this process. We are allowing customers who are using Nessus Professional or Manager to migrate their configuration easily into Tenable Vulnerability Management.
- **Additional improvements include:**
  - Exposing additional audit trail configurations to advanced settings.
  - Option to adjust log levels without requiring a restart of the service.

Bug Fixes

- Resolved issue where plugin script timeouts were not working when set to 0.
- Resolved issue where Tenable Security Center was receiving unexpected 500 Responses when querying Agent scan results from Nessus Manager.
- Resolved issue where Audit scans were failing in Tenable Vulnerability Management when Asset Isolation was enabled.
- Resolved issue where diff CSV exports in Nessus Manager were blank.
- Resolved issue where large PDF exports were timing out.

Nessus 8.2.1 Release Notes - 1/24/2019

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.2.1.

Bug Fixes

- Fixed issue where hostname-based exclusion rules caused all hosts to be rejected for Tenable Vulnerability Management linked scanners.

Nessus 8.2.2 Release Notes - 1/31/2019

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Fixed issue where plugin timeouts were not being honored, causing some scans to not complete for several days.
- Fixed issue where SecurityCenter UI was displaying all scanned hosts as dead, even though scan results were correct.
- Fixed an XSS issue when viewing scan configuration policies.

Note: For information on fixed vulnerabilities, see https://www.tenable.com/security/tns-2019-01.

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.2.2.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Upgrading to Nessus 8.2.2 will trigger a rebuild of your plugin database. This may take several minutes to complete.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.2.3 Release Notes - 2/17/2019

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- The previous version was incorrectly signed with the wrong key, which could lead to unexpected application feature flags being enabled in isolated cases. The issue did not affect scan performance or results.

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.2.3.

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Upgrading to Nessus 8.2.3 will trigger a rebuild of your plugin database. This may take several minutes to complete.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.3.0 Release Notes - 2019-03-26

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

> **Note:** For Nessus 8.3.0 scanners installed on Windows, set the new setting **Max Plugin Output Size** to 100000 to ensure that scan exports function correctly. You can configure this setting in the **Scanning** section of Advanced Settings. For more information, see the Knowledge Article Nessus Scanner on version 8.3.0 restarts upon scan completion. This was fixed in version 8.3.1.

New Features

The following are the new features included in the Nessus 8.3.0 Release:

- **Flexibility for Reporting in Nessus Professional** - Often there can be too much data; now Nessus enables you to select precisely which information is included when exporting PDF and HTML reports. As an example, a user can choose when exporting to only include the host information, vulnerability information, and vulnerability score when creating a report. The user can also select to save the export options as default for any subsequent exports.
- **Performance updates for Agent deployments using Nessus Manager** - Tenable made improvements to the processing time for scan results on Nessus Manager. The update

includes disabling the inclusion of Audit Trail and KB data by default. As a best practice, it is recommended leaving these disabled for production environments. For testing/troubleshooting, both abilities can be re-activated for smaller agent groups if needed.

  - Additionally, new options to optimize agent data merge performance can be configured if desired and can provide additional speed-up. See the Agent Advanced Settings documentation for details on configuring these optimizations.

- **Scan Template Updates** - Similar to plugin updates, scan templates can be updated at various times. With this release, new policies and policy updates are now delivered automatically.

- **Additional improvements include** -

  - Added the ability to update the Offline registration license in the Nessus UI for scanners registered offline.

  - Add a new Advanced Setting `plugin_output_max_size_kb`, defaulted to 1MB, to configure the maximum per-plugin output size for XML elements in .nessus reports.

  - Added various NASL improvements and bug fixes

Bug Fixes

- Fixed an issue with filtering Scan Results on a date field that was causing missing results, due to a bad regular expression match.

- Fixed an issue with importing Agent results by updating XML report processing to remove all invalid characters from XML.

- Fixed an issue where incorrect date format of yy-mm-dd instead of YYYY-mm-dd was appearing in some places in the UI.

- Fixed an issue with ARP Discovery.

- Fixed an issue with importing Advanced Agent scans that was causing all plugins to be enabled in the imported scan.

- Fixed an issue where customer hostnames containing invalid XML characters were breaking scan exports.

- Fixed an issue with CSV Report Line Terminations, change cause reports doubling in size.

- Fixed an issue with Plugin dependency processing that was causing empty results when running offline configuration audits from a Nessus scanner installed on a Tenable Appliance.
- Fixed an issue with exporting Scan Diffs.
- Fixed an issue where color-coded severity bullets were not displayed for Nessus PDF reports.
- Fixed an issue with importing very large scan results into Tenable Security Center.
- Fixed an issue that was causing extraneous error messages in the nessusd.dump log file.
- Updated openSSL patch level 1.0.2r to ensure latest security fixes are available. For more information, see the security advisory.

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.3.0.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Upgrading to Nessus 8.3.0 will trigger a rebuild of your plugin database. This may take several minutes to complete.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.3.1 Release Notes - 2019-03-29

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: For a summary of the new features introduced in Nessus 8.3.0, see the Nessus 8.3.0 Release Notes - 2019-03-26.

Bug Fixes

- Fixed issue with 8.3.0 Windows scanners occasionally failing on scan export by increasing the default value for the "Max Plugin Output Size" setting to 100MB. (See KB article: https://community.tenable.com/s/article/Nessus-Scanner-restarts-upon-scan-completion).

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.3.1.

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Upgrading to Nessus 8.3.1 will trigger a rebuild of your plugin database. This may take several minutes to complete.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.3.2 Release Notes - 2019-04-30

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

Bug Fix	Defect ID
Fixed issue with plugin output truncation in .nessus reports	00783120, 00782321
Fixed issue with the changing of a reported hostname to the FQDN of the target in the presence of certain Tenable Vulnerability Management exclusion rules	00783297, 00765880
Fixed issue with Nessus instances crashing in Windows	00753926, 00745234, 00766928, 00758204, 00768384, 00752934, 00769286, 00759233, 00770668,

	00752487, 00773830, 00775359, 00773072, 00770266, 00762859, 00774515, 00782586, 00782269, 00785051, 00786504
Fixed issue with defragmentation of plugin databases	00732200
Fixed issue with slow enumeration of exclusion lists during plugin enablement	00746945

Nessus 8.4.0 Release Notes - 2019-05-14

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Nessus 8.4.0:

- **Introducing Nessus Essentials -** Nessus Essentials is a free vulnerability scanner for up to 16 IPs that provides an entry point for users into the Tenable ecosystem. Backed by market leading functionality from Nessus Professional, Nessus Essentials gives you the accuracy and speed you need to discover, prioritize and remediate vulnerabilities. Ideal for educators, students and individuals starting their cyber security careers, Nessus Essentials helps you get started with vulnerability assessment.
- **Updates to UI -** Branding has been updated throughout the product along with some minor improvements to UI.

- **Enhanced CSV export capability -** Users can now select which fields to include as part of their CSV exports. If needed, users can revert to the default export settings.
- **Agent Blackout Windows -** The definition of blackout windows in Nessus Manager for agents is being extended with increased granularity. With this feature, blackout windows become more flexible by allowing customers to select specifically which activity is allowed and disallowed during a blackout window.

Bug Fixes

- Fixed issue with NFS plugin not properly detecting mountable drives.
- Fixed issue with plugin output attachments not opening correctly in some cases.
- Fixed issue with disappearing scan result search filter when no result is returned by filter.
- Fixed issue with filters not applying correctly on certain Nessus reports.
- Fixed intermittent issue with reports not including all expected content.
- Fixed issue with the nessuscli command producing a benign warning.
- Fixed issue with ssl_cipher_list advanced setting not being honored.
- Fixed issue with Nessus installation of templates that cross multiple filesystems.
- Fixed a number of UI presentation issues.

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.4.0.

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- Upgrading to Nessus 8.4.0 will trigger a rebuild of your plugin database. This may take several minutes to complete.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.5.0 Release Notes - 2019-06-25

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: For customers managing Nessus Agents through the Nessus user interface, there is a bug when viewing filtered Agents. If you apply a filter and select the **Select All** check box, any action will occur against *all* Agents, not only the ones displayed. This could cause all linked Agents to inadvertently be unlinked. A fix is available in Nessus 8.5.1.

New Features

The following are the new features included in Nessus 8.5.0:

- **Nessus Essentials streamlined activation and registration** - The activation and registration process has been simplified. Users can now register and activate Nessus Essentials directly from the application. Users can now upgrade from Nessus Essentials to Nessus Professional directly from the application as well.
- **Nessus report filtering enhancements** - Creating reports for selected hosts and vulnerabilities has been made faster and more intuitive. Users can generate reports quickly and easily by selecting items and choosing "Report," without the need to first build filters. In addition the Report action has been separated from the Export action to make the difference between the two more clear.
- **Removed IP license restrictions for Host Discovery scanning** - Nessus Essentials and Nessus Professional trial customers can now perform Host Discovery scans against their full network ranges without encountering IP limits based on their license.
- **License expiration grace period changes** - Updated license expiration behavior. Scanning will be disabled upon license expiration, however users will have a 30 day grace period to access the application and review scan results that have already been generated.
- **Performance improvements** - Scan results should present noticeably faster and agent management should be more responsive.

Bug Fixes

Bug Fix	Defect ID
Fixed issue with Security Center hanging when processing certain types of	00672350

scans	
Fixed intermittent issue with Security Center when scanning specific host	00693416
Fixed issue with missing agent name in scan notes under specific conditions	00642561
Fixed issue with enabling plugins in filtered results not always behaving as expected	00757135
Fixed issue with license expiration date presentation	00774205
Fixed a number of issues with Nessus API documentation	n/a
Fixed an issue where template files could have mismatched signatures when upgrading under certain conditions	n/a
Fixed an issue with Nessus not properly setting Cache-Control and Expires headers.	n/a
Fixed an intermittent issue with a migration error being generated when installing under certain conditions	n/a
Fixed an issue with unnecessary sorting icon being shown in Advanced Settings	n/a
Fixed an issue with incorrect error notification being shown when required fields are not populated in policies	n/a
Fixed an issue where the user is presented with a red invalid box before entering in any information when using Internet Explorer	n/a
Fixed an issue where filter values are reset to default under certain conditions in the Vulnerabilities view	n/a
Fixed an issue with notifications overlapping UI elements when messages are verbose	n/a
Fixed an issue where inputs were not sanitizing white space properly	n/a
Fixed an issue with maximum values for Plugin output causing unexpected behavior	n/a
Fixed an issue with incorrect default port being set for Scanners when	n/a

managed by Industrial Security	
Fixed intermittent issue with paused scans not appearing to fully complete	n/a

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.5.0.

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus 8.5.1 Release Notes - 2019-07-02

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

> **Note:** For a summary of the new features introduced in Nessus 8.5.0, see Nessus 8.5.0 Release Notes - 2019-06-25.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where Agent filter options no longer include "none" when filtering by "Member of Group."	00834584
Fixed an issue where the "Select All" check box ignores filter on Agents list page.	00834666

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.5.1.

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus 8.5.2 Release Notes - 2019-08-05

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: For a summary of the new features introduced in Nessus 8.5.0, see Nessus 8.5.0 Release Notes - 2019-06-25.

Bug Fixes

Bug Fix
Fixed an issue with plugin size causing a significant impact on feed updates and scanning on Nessus scanners.

Upgrade Notes

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.5.2.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus 8.6.0 Release Notes - 2019-08-13

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- **In-Product Notification Enhancements** - Improved license expiration notifications to provide license-specific renewal links. Added the capability to permanently dismiss notifications that have been viewed. Added a notification history page to allow users to review previous notifications.

- **Watermarked reports for Nessus Essentials and Nessus Pro Trials** - Added watermarks to exported reports for Nessus Essentials and Nessus Pro evaluations.

- **Enterprise Supportability: Scan and Policy Ownership** - Our enterprise users of Nessus often have personnel changes that require them to change or remove users from their system. This feature allows administrators to claim ownership of user content.
- **Telemetry Enhancements** - Added an advanced setting that allows users to opt out of providing telemetry reporting back to Tenable. Telemetry information ensures that users will benefit from more intuitive and useful features and capabilities in future Nessus releases. Please refer to the documentation describing advanced settings for more information.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where users were unable to filter the agent list by IP address in Nessus Manager	00832160
Fixed an issue with exporting HTML custom reports containing non-standard character sets	00775714
Fixed an issue where multi-homed machines would not honor the forced source IP command	00801670
Fixed an issue with scan result filters no longer accepting a comma delimited list of values	00832101, 00833265
Fixed an issue when attempting to add agents by search results to agent groups	00832160
Fixed an issue where plugin attributes were no longer included in .nessus files sent to T.sc, by adding a config setting to re-enable the attributes	00840184, 00848793
Fixed an issue where the scanner health page does not appear to display CPU usage correctly	N/A
Fixed an issue with scan plugin filters	N/A
Fixed an intermittent issue with displaying records in the Vulnerabilities view	N/A
Fixed a number of UI presentation issues	N/A
Fixed typo in the advanced settings for Max HTTP Connections	N/A

Fixed an intermittent issue with Agent 'status' on Agent Detail page is not displaying state correctly	N/A
Fixed an issue where 'Plugin Family' filter is not working as expected and showing "no result found"	N/A
Fixed an issue with agent group deletion work flow	N/A
Fixed an issue where search agent count is not displaying correctly	N/A
Fixed an issue where search functionality wasn't as inclusive as expected	N/A
Fixed an issue where unlicensed scanners show as "expired"	N/A
Updated OpenSSL version to 1.0.2s.	N/A
Fixed a potential issue in XMLRPC API affecting Windows installations	N/A

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus 8.7.0 Release Notes - 2019-09-24

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- **Nessus Manager Clustering Enhancements:** Support for agent migration into Nessus Manager clusters is now available. Clustering no longer requires a licensing flag, and is available to be configured for all customers using Nessus Manager for large agent installations.
- **Tenable Research News Widget:** In Nessus Essentials, RSS feed-based notifications present recent publications from Tenable Research in the UI, providing a live view of the ongoing research and publications of Tenable's cutting-edge Research organization.
- **Host Discovery Scan Wizard:** New users of Nessus Essentials and Nessus Professional trial are presented with a scan wizard upon first use of the product to walk through the process

from host discovery to vulnerability scanning. Now it only takes a couple clicks for new users to create and execute their first scan.

- **Licensing transparency for Nessus Essentials and Nessus Professional Trial:** A new License Utilization page gives Nessus Essentials and Nessus Professional trial users visibility into the hosts that have consumed their licensed pool of hosts, as well as the length of time before each asset will no longer count against the license.
- **Updated Host Discovery Results Page**: Refreshed the results page for Host Discovery Scans to present more relevant information. Users can now see port, host, and OS information when available, based on the type of discovery scan performed.
- **Launch scans from result set of another scan:** Users can now select hosts from one scan result set to open or launch a new scan with those hosts pre-populated as targets.
- **Scan templates have been grouped by type:** Scan templates have now been grouped by type and will fall into one of the following categories: Discovery, Vulnerability, and Compliance.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where all agent filters are removed when removing just one.	00842212
Fixed an issue with Nessus compliance filters returning zero results.	00845952
Fixed an issue where Nessus Manager blackout window was not being enforced.	00815692
Fixed an intermittent issue where a scan ran outside of the scheduled scan time when daylight savings time started.	00713482
Fixed an issue where managed scanners were displaying templates that are only available through Tenable Vulnerability Management.	00823897
Fixed an issue where the re-balance button for clustering was not always responsive on first pass.	00831948
Fixed an issue where disabled scans may not run after being re-enabled.	00836620
Fixed an issue where the unread/read scan(s) indicator in the UI was sometimes incorrect.	00845172, 00854997,

	00847274
Documented the possible agent status values returned from the Nessus/Agents API in the online API documentation.	00850459

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus 8.7.1 Release Notes - 2019-09-26

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

Bug Fix	Defect ID
Fix issue with Windows scanners being unresponsive after auto-upgrade to Nessus 8.7.0.	00886021

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.7.2 Release Notes - 2019-10-10

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- **International Character Display:** Added ability to properly store and display international characters in Nessus scan results.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where Tenable Vulnerability Management linked scanners had intermittent SSL errors if they could not reach ocsp.digicert.com.	-

Upgrade Notes

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Nessus 8.8.0 Release Notes - 2019-11-05

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Nessus 8.8.0:

- **Red Hat 8 Support** - Nessus now supports Red Hat 8 as a supported host operating system.
- **Agent key update confirmation** - A confirmation prompt now appears when a user attempts to update the Nessus Agent key.

Changed Functionality and Performance Enhancements

The following are changes to functionality included in Nessus 8.8.0:

Change	Defect ID
Log rotation max_files default change - The default value for number of log files retained when rotating logs has changed from 100 to 10. This change applies to backend.log and www_server.log files, and will cause the oldest files to be rotated off if the new maximum is exceeded. Customers can modify the number of log files retained by changing the setting in the log.json file. For more information, see Manage Logs in *Tenable Nessus User Guide*.	00903832

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where ping doesn't work in a static route network environment	00792741
Fixed an issue where some appliances were consuming their available disk space with logs by reducing the default log rotation Max_Files value to 10	00903832
Fixed an intermittent issue where blackout windows were not enforced by Nessus Manager	00815692
Fixed an intermittent issue where agent policies may have been missing a selected tag	00867327
Fixed a presentation issue in the UI with very long folder names	00871572
Fixed an issue where blackout windows were not enforced immediately after 00:00	00815692
Fixed an issue where an agent unlinked from UI cannot relink from agent CLI	-
Fixed an intermittent issue with heartbeats not properly timing out in the NASL recv() function	00759300

Upgrade Notes

- For Nessus 8.8.0 and later running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. The following Windows versions require a minimum Service Pack to be installed:

  - Windows 7 SP1
  - Windows Server 2008 SP2
  - Windows Server 2008 R2 SP1

- You can upgrade to the latest version of Tenable Nessus from any previously supported version.
- If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

2018 Tenable Nessus

Nessus 7.0.1 Release Notes - 1/11/2018

Nessus 7.0.2 Release Notes - 2/13/2018

Nessus 7.0.3 Release Notes - 3/14/2018

Nessus 7.1.0 Release Notes - 5/15/2018

Nessus 7.1.1 Release Notes - 6/13/2018

Nessus 7.1.2 Release Notes - 6/26/2018

Nessus 7.1.3 Release Notes - 7/31/2018

Nessus 7.1.4 Release Notes - 12/19/2018

Nessus 7.1.5 Release Notes - 2019-08-08

Nessus 7.2.0 Release Notes - 8/27/2018

Nessus 7.2.1 Release Notes - 10/11/2018

Nessus 7.2.2 Release Notes - 11/08/2018

Nessus 7.2.3 Release Notes - 2019-08-08

Nessus 8.0.0 Release Notes - 10/23/2018

Nessus 8.0.1 Release Notes - 11/01/2018

[Nessus 8.1.0 Release Notes - 12/4/2018](#)

[Nessus 8.1.1 Release Notes - 12/19/2018](#)

Nessus 7.0.1 Release Notes - 1/11/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle [Matrix](#) and [Policy](#).

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes & Improvements

- Meltdown / Spectre Policy Template
- Unable to deselect option "Verify SSL Certificate" in Nessus 7
- Nessus v7 cannot save credentials on IE 11

File Names & MD5 Checksums

File	MD5
NessusAgent-7.0.1-amzn.x86_64.rpm	cdb717380ed440f23cd6b0c6a453ea42
Nessus-7.0.1-amzn.x86_64.rpm	c745663244dd421e3970cd081a5f98d6
NessusAgent-7.0.1-debian6_amd64.deb	fdd66af6828b524c190414ced4156e59
Nessus-7.0.1-debian6_amd64.deb	6aa52a586457e38fa46722b1c226f0c3
NessusAgent-7.0.1-debian6_i386.deb	0606ddd905e5320a70f32e630f402a3e
Nessus-7.0.1-debian6_i386.deb	47cbde05a80718ca849a1432f52cf55f
NessusAgent-7.0.1-es5.x86_64.rpm	80e2d2696ceb4f40ffe61e16b48f1ed8
Nessus-7.0.1-es5.x86_64.rpm	d38c5c95486f67593a8494b3d01e8426
NessusAgent-7.0.1-es5.i386.rpm	a13d8d379efae9b7becfa4c8228dc958
Nessus-7.0.1-es5.i386.rpm	b1fa129487496c442db0ecfc15fe1e26

File	MD5
NessusAgent-7.0.1-es6.x86_64.rpm	cd798010aabe6d1c30a92f665f8a3993
Nessus-7.0.1-es6.x86_64.rpm	e3acc13a9d32e7583426a144b74965b4
NessusAgent-7.0.1-es6.i386.rpm	786595a792626bec85dcbebc41790ded
Nessus-7.0.1-es6.i386.rpm	8aa5af9003de6e220e68a62d86c08f03
NessusAgent-7.0.1-es7.x86_64.rpm	91766d919a982d8df8ed0a0130255b63
Nessus-7.0.1-es7.x86_64.rpm	c822d69fcfdfcee02ad9f71629a78520
Nessus-7.0.1-fbsd10-amd64.txz	a8a3a34ef22eb164d87a9a018905dd99
NessusAgent-7.0.1-fc20.x86_64.rpm	35d46ef591c4fb6d91605f750e32f27a
Nessus-7.0.1-fc20.x86_64.rpm	1ef0611567487dd891d43814018922fe
NessusAgent-7.0.1.dmg	95634e68b7c367926a5f7f7a8abc6c0b
Nessus-7.0.1.dmg	1fa2e5b4b30bea3a58ffd0938383cc41
NessusAgent-7.0.1-suse11.x86_64.rpm	9a031a3e67f718d7aa7a676c6b6ff5db
Nessus-7.0.1-suse11.x86_64.rpm	0248838f85eb6347a50cd33b16eff56e
NessusAgent-7.0.1-suse11.i586.rpm	ec07edf476ed851d180d8a3f7409d435
Nessus-7.0.1-suse11.i586.rpm	254caabbece77805a9de667a6eec3782
NessusAgent-7.0.1-suse12.x86_64.rpm	a679d1ae6cf22797dfcddff70454f312
Nessus-7.0.1-suse12.x86_64.rpm	5545af934bc8c96f41e2af49abb5eab3
NessusAgent-7.0.1-ubuntu1110_amd64.deb	9bb099d9765f8361023087b5472cb2e7
Nessus-7.0.1-ubuntu1110_amd64.deb	149f359efbe852dd54e7c6002866db68
NessusAgent-7.0.1-ubuntu1110_i386.deb	552c3b2130bd0a04514d6dcef0781e4e
Nessus-7.0.1-ubuntu1110_i386.deb	28ac72f3c957965b5b7aa0e105267898
NessusAgent-7.0.1-ubuntu910_amd64.deb	0325e32947663b792d4673e73689c85f

File	MD5
Nessus-7.0.1-ubuntu910_amd64.deb	6aaac7fe980d5317fe080d212c7497d0
NessusAgent-7.0.1-ubuntu910_i386.deb	60b405742bccc5ce175329978f5c1bb8
Nessus-7.0.1-ubuntu910_i386.deb	0d0228553b6768e35fb140e4179f2622
NessusAgent-7.0.1-Win32.msi	82730052a7f4cf666206ca1c70c0462c
NessusAgent-7.0.1-x64.msi	f731d76ecb71a7acacb364ef0421b470
Nessus-7.0.1-Win32.msi	d81e34851421a2f2ad4c577ddde647ef
Nessus-7.0.1-x64.msi	5edbebe240cc84222a3dad5d172283bd

Nessus 7.0.2 Release Notes - 2/13/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes & Improvements

- License transfer for Pro v7 users only
- Active license visibility
- Competing banner improvements
- Reinstate API functions related to integrations
- Updates to Nessus to support CyberArk certificate authentication
- Nessus Manager v7 not saving/using su creds
- Update GPG key expiration
- Plugin status should persist after edit
- Browser compatibility test triggers security exception in non-IE, javascript error on IE 11/Edge

- Built in API docs shouldn’t display the restricted APIs
- Scheduled scans created via API don’t start as scheduled
- Issues with custom logo in report emails
- Nessus 7: Adding second audit file autofills the first audit file
- Custom reports showed up on non-opted-in upgraded Nessus Pro
- Everytime nessusd restarts, we check the feed for core updates even though the setting is disabled for offline updates
- Cisco enable password bug in policy editor

File Names & MD5 Checksums

File	MD5
Nessus-7.0.2-x64.msi	7621d0f7d4c61d42b5327a03c956959c
Nessus-7.0.2-amzn.x86_64.rpm	4bc90e8438d918208e1a23b78164c21c
Nessus-7.0.2-Win32.msi	9b8c6525a0a2226633867fdc6badbb47
Nessus-7.0.2.dmg	e7280e271d0ffacb5ed38fc274dcb389
Nessus-7.0.2-es5.x86_64.rpm	2d736b4aee9e54032bc6262d73a14a0a
Nessus-7.0.2-es5.i386.rpm	0a7a91a375c21518c638663409388495
Nessus-7.0.2-es6.i386.rpm	d29962289435a2f7cd7f503c2c4fcebb
Nessus-7.0.2-fbsd10-amd64.txz	893052285743eb9b97404622d131d7ff
Nessus-7.0.2-ubuntu1110_amd64.deb	a5c6dbc37c792e5b6fdfe5a880906113
Nessus-7.0.2-ubuntu1110_i386.deb	6735f029063cc0a5fc0d3316b7e19022
nessus-updates-7.0.2.tar.gz	19c509e82c2742fdc84628531160ae26
Nessus-7.0.2-debian6_amd64.deb	58fcc745dc9e756ff40a29e15a52f205
Nessus-7.0.2-debian6_i386.deb	ed0366cdb01e9a2aac8295a2582350b9
Nessus-7.0.2-es6.x86_64.rpm	f50a861b41a1df78f29042f109af881a

File	MD5
Nessus-7.0.2-es7.x86_64.rpm	16df36d86bec9aeaf3dcc1e82834311c
Nessus-7.0.2-fc20.x86_64.rpm	0bbf1879d13a1ddd2667eede1468e553
Nessus-7.0.2-suse11.x86_64.rpm	8298fe210d35df0672d264238c98419c
Nessus-7.0.2-suse11.i586.rpm	d66a61888a2c94d25728c42b33bbbd00
Nessus-7.0.2-suse12.x86_64.rpm	1dd817c6d32455cef06a410918fe82b5
Nessus-7.0.2-ubuntu910_amd64.deb	06f234bcc339caa40129e6f1b57531bb
Nessus-7.0.2-ubuntu910_i386.deb	b5cfc60f48dd06f245a2a379dd195a0b

Nessus 7.0.3 Release Notes - 3/14/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New

The following are new features available with Nessus 7.0.3:

- Ability to use BeyondTrust PasswordSafe as a credential source for Windows and SSH credentials

Bug Fixes & Improvements

- In Nessus Manager, CyberArk credentials now successfully save when a certificate is not attached.
- Nessus Manager now processes agent results that were submitted while the scan window was open as opposed to halting processing when the scan window finishes. Customers who are using Nessus Manager for agent management may need to re-evaluate their synchronization schedule based on this change.

File Names & MD5 Checksums

File	MD5
Nessus-7.0.3-fbsd10-amd64.txz	9f3bc8cbbd7bddb358f24668188ad7aa
Nessus-7.0.3-es5.x86_64.rpm	78440d81c26111f58934364953ea217d
Nessus-7.0.3-debian6_amd64.deb	a3788a527ffd464e75dc0288afad0250
Nessus-7.0.3-x64.msi	6d8d5cf227402400b3191aa63a9d09f5
Nessus-7.0.3-Win32.msi	fae3fe3fdc21a3bffa83d4a5f45a8b9a
Nessus-7.0.3.dmg	d03e16c2e2fd693ea3076db6917b86b6
Nessus-7.0.3-debian6_i386.deb	a6939e675e18797b064ef1b4871e1cea
Nessus-7.0.3-es5.i386.rpm	247ec891caccd48ee3880fb22ff75f1f
Nessus-7.0.3-es6.x86_64.rpm	26ec2b6d237fe6c7d1cd9a8caf8d4d46
Nessus-7.0.3-es6.i386.rpm	5fef1804e5e8b87d023e59d633440cc1
Nessus-7.0.3-es7.x86_64.rpm	3da6e480ed65f641f8304bf31c503dcd
Nessus-7.0.3-fc20.x86_64.rpm	384ceff2344f2e3a146d14ba149a4788
Nessus-7.0.3-ubuntu1110_amd64.deb	8944c9b570a84662503934d4fde0a2bd
Nessus-7.0.3-suse11.x86_64.rpm	33d9804e738c981b886d7d19b60c18ec
Nessus-7.0.3-suse11.i586.rpm	e4541dd0f60e0f96bb06a5e971b8bd0c
Nessus-7.0.3-suse12.x86_64.rpm	18889ac011da822ce68b08bb237a3903
Nessus-7.0.3-ubuntu1110_i386.deb	93c6d2213abe4e28443941dfc4a12578
Nessus-7.0.3-ubuntu910_amd64.deb	6569ac6d247c6d5e4ba0257ec440be39
Nessus-7.0.3-ubuntu910_i386.deb	d94f079becdaa4d5f780b48a384bc03d
Nessus-7.0.3-amzn.x86_64.rpm	79b1f2ff0a8ce302f581d9465417d2f3
nessus-updates-7.0.3.tar.gz	d0eb093c32ff9ca727e312d57655275f

Nessus 7.1.0 Release Notes - 5/15/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New

The following are new features available with Nessus 7.1.0:

- Nessus Professional to Tenable Vulnerability Management Upgrade Assistant
- Improved Nessus password complexity and management
- Purchase link added to Nessus Eval

Bug Fixes & Improvements

- Scan Details of Shared Scan Do Not Contain Scanner
- Nessus API - "FREQ=ONCE" & "FREQ=ONETIME"
- Nessus 7.0.x not showing plugins in right windows with multiple filters enabled
- Agent scan results not being processed
- Nessus only lists the ipv4 address for the first 100 interfaces
- Proxy isn't enabled when configured through UI
- Missing Plugin in Meltdown/Spectre template
- Session Management Vulnerability in Nessus
- Agent filtering shows incorrect '+' icons
- Nessus Web Server version in SecurityCenter details section shows 5.0.0
- Entering incorrect master password appears to succeed
- Proxy - Required fields that are missing should be marked red when hitting save
- Scrollbar in compliance tab hides audit counts
- Error Text Missing location for OSX

- Nessus vulnerable to cross-site scripting
- Editor wrongfully claims an offline config is required for audits
- Non-default scan window yields input box + drop down
- Software update banner does not work from Settings->About page
- Attempting to disable Dashboard, re-enables them
- Agent API documentation fixes

File Names & MD5 Checksums

File	MD5
Nessus-7.1.0-amzn.x86_64.rpm	11a61a6708ca0af3566e08b4b2c09baf
Nessus-7.1.0-debian6_amd64.deb	b1975e2719053aa59a5e728de3962d45
Nessus-7.1.0-debian6_i386.deb	236d7633f47dd19b88347aa8013abf24
Nessus-7.1.0-es5.i386.rpm	834506b0c1a33fb98d6831c5c5a77e08
Nessus-7.1.0-es5.x86_64.rpm	ce483dc0f86351d0399c5fdcf51eacd2
Nessus-7.1.0-es6.i386.rpm	f09fe89935b3df6a5b540198f57471a4
Nessus-7.1.0-es6.x86_64.rpm	829affd8b400ad893b358ef200264728
Nessus-7.1.0-es7.x86_64.rpm	ad97a0a8914bbe96bcda2626f2f8fdad
Nessus-7.1.0-fbsd10-amd64.txz	1c4bacbc4ab2cd13be249b3b1f69e9ce
Nessus-7.1.0-fc20.x86_64.rpm	e389acaf961eeda6cc3df8d62297de04
Nessus-7.1.0-suse11.i586.rpm	f05378d05911c9e4be5855560fc53739
Nessus-7.1.0-suse11.x86_64.rpm	17808087163c49c7ba95a023a0a042d9
Nessus-7.1.0-suse12.x86_64.rpm	3d7ae08a810ceba534bdc0da67025b13
Nessus-7.1.0-ubuntu1110_amd64.deb	9ee00d818edd95d285106ce323d93c9d
Nessus-7.1.0-ubuntu1110_i386.deb	f1c3a3b61dd0ad11485e34dfd65268b8
Nessus-7.1.0-ubuntu910_amd64.deb	c722043c56452e519371593d9ba78bf3

File	MD5
Nessus-7.1.0-ubuntu910_i386.deb	a314f6afae1fd40d3bd0a948abcfd83c
Nessus-7.1.0-Win32.msi	08646615c7774b3f1abe6898020bd45a
Nessus-7.1.0-x64.msi	27660e43f6fe541fe16ebdc5f25eb051
Nessus-7.1.0.dmg	ad88bb22d68c59cbacbfc3365a3ebf9c

Nessus 7.1.1 Release Notes - 6/13/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New

- Automatically update the hostname of an agent in Nessus Manager when it changes. This feature allows the agent hostname to be updated automatically instead of requiring the agent to be unlinked and relinked. This requires the "update_hostname" parameter to be set to "yes" on the agent, and requires Nessus Agent 7.1.0.
- Export full list of agents via the Nessus Manager UI. This provides customers, who do not leverage the Nessus API, the ability to export the agent details as a .csv report for use.
- Track agents and attributes after unlinking. This provides users the ability to continue tracking unlinked agents and associated details. This is an opt-in feature and requires Nessus Agent 7.1.0.
- Automatically maintain unique agents in Nessus Manager. This eliminates situations where multiple entries for the same agent can appear in Nessus Manager. This requires Nessus Agent 7.1.0.
- Updated third-party libraries with known vulnerabilities, see the security advisory for more information.

Bug Fixes & Improvements

- Agent linked and unlinked status is visible in the Nessus Manager UI.
- Re-installation can remove previous installation data.
- Fixed error message that appeared during latest install of Nessus Manager.
- Unlinked Agents won't count against licenses limit when scanning.
- Fixed unlink button on Agent details page.
- Fixed unlinked Agents counting against Agent total.
- Delete Agents token from db when unlinking an Agent.
- Fixed inappropriate error notification on setting "Unlink inactive agents after" greater than 90.
- Fixed inconsistent Error When Unlink Day > Remove Days.

File Names & MD5 Checksums

File	MD5
Nessus-7.1.1-amzn.x86_64.rpm	d451e5b1afd0b4243f6fd2d1c3116f7b
Nessus-7.1.1-debian6_amd64.deb	1d4cc21b62f4d327260bab77fe1e6fdc
Nessus-7.1.1-debian6_i386.deb	0781e34108ade9478ffcb3f06e736dff
Nessus-7.1.1-es5.x86_64.rpm	f58dfdaa22bd683cec24cc9f81f518f6
Nessus-7.1.1-es5.i386.rpm	0e2ea40eaba90aa38fd441b3610c112d
Nessus-7.1.1-es6.x86_64.rpm	d1cc3eda39c35c1a3efb39601b229182
Nessus-7.1.1-es6.i386.rpm	466ec5842b7468e5e2b7dcb07805d041
Nessus-7.1.1-es7.x86_64.rpm	f7f5d443c9744e25249dcd8b61bf86cc
Nessus-7.1.1-fbsd10-amd64.txz	b20f3a30d7b65d61d15136a92363f090
Nessus-7.1.1-fc20.x86_64.rpm	8c1d9f1829bccd945c39315bfe246a18
Nessus-7.1.1.dmg	330fdea4102a4a2fef0a417b7cd1eb16
Nessus-7.1.1-suse11.x86_64.rpm	aa72ea893f72524192f93a0c7b73f593
Nessus-7.1.1-suse11.i586.rpm	71fd514fc3fd6f590737e6d880f98411

File	MD5
Nessus-7.1.1-suse12.x86_64.rpm	8ee137a351638ee91fdd551f9186dc93
Nessus-7.1.1-ubuntu1110_amd64.deb	1a8bef01ef8f3fcfe2f6846c57404e05
Nessus-7.1.1-ubuntu1110_i386.deb	2e3ecf199795e9e52c127cd56e6ffb08
Nessus-7.1.1-ubuntu910_amd64.deb	d9f08072f7d049763acdf58c01343590
Nessus-7.1.1-ubuntu910_i386.deb	805aef4c8223e2808662a097e158233f
Nessus-7.1.1-Win32.msi	e8d1f793eb94878138f2ca1ca99839db
Nessus-7.1.1-x64.msi	7b4904e176b3f15bd3b7e2a1ae2fd4d2

Nessus 7.1.2 Release Notes - 6/26/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New

- Ability to limit the amount of scan history that's retained - Nessus users will now have the ability to set a limit on how much scan history, in days, is kept. This will help Nessus users manage disk usage.
- Change link of Nessus scanner from Security Center to Tenable Vulnerability Management - Tenable Security Center users can now change the link destination of a Nessus Scanner to Tenable Vulnerability Management within the UI of a Nessus Managed scanner.

Bug Fixes & Improvements

- Master Agreement updated for Nessus Pro/Home/Eval users.
- On an existing policy, enabling one plugin will end up enabling the entire family.

- When creating a scan from an Audit Cloud Infrastructure Template Policy, it forces Targets to be specified, preventing proper scanning.
- Apple Mail unable to render HTML email from Nessus.
- "Select All" check-box is checked by default in 2nd page in pagination.
- Deprecated audits should generate a scan note.
- Blank result shown in Advance Scan >> Plugins even if "service detection" is enabled.
- New Scan is created with empty name (Use Space bar key) if we create scan from User Defined policies whereas normal scan is not created using spaces.
- Updated Nessus password storage to use a secure / slow algorithm like PBKDF2.
- Plugin Editor when show enabled, disable plugins won't show the rest plugins.
- 'More' button's options are not loading when user directly click on 'select All' check-box and click on 'More' button.
- ‘More’ button is NOT displayed on second page to remove selected scans from first page.
- Selected counts are not matched with Selected items when user un-check the check-all box and validate selected items on first page.
- Under Scans/Policies >> Plugins, Plugin family status is not getting changed to “ENABLED” if user has applied the filter and changes disabled plugin to enabled from the right side of the plugin list.
- 'Selected count' are NOT getting cleared if user first click on 'Select All <Count>' link and then click 'Clear selected Items' link.

File Names & MD5 Checksums

File	MD5
Nessus-7.1.2-amzn.x86_64.rpm	c9c1288b527040f069d30fe658d6e7e1
Nessus-7.1.2-debian6_amd64.deb	e6aac5f29235527c50d9f91bdd1c754d
Nessus-7.1.2-debian6_i386.deb	6ce416cc4178be84ed31daf6caf3410e
Nessus-7.1.2-es5.x86_64.rpm	52a9cbd36b443ecb095ce4bfa7f26530
Nessus-7.1.2-es5.i386.rpm	6a8300056fd0b134d460487712b028fb

File	MD5
Nessus-7.1.2-es6.x86_64.rpm	cdac0129251e99c4cc2bf08b577430cf
Nessus-7.1.2-es6.i386.rpm	a8f13a606c82cf40776d639c0dfa3cd9
Nessus-7.1.2-es7.x86_64.rpm	18692cd7693dd83e29278097ff2d0a97
Nessus-7.1.2-fbsd10-amd64.txz	ca17f46599282497295bc4c09b602fbc
Nessus-7.1.2-fc20.x86_64.rpm	002f12ee8063eaceef7d7f1e64739308
Nessus-7.1.2.dmg	02444184b30d43545f6f9e9209188f1d
Nessus-7.1.2-suse11.x86_64.rpm	4a7ca9b29979ce5204df68cf95848408
Nessus-7.1.2-suse11.i586.rpm	762441750b907662ba6def2a9237a10d
Nessus-7.1.2-suse12.x86_64.rpm	3a8d3b0d660804df5a29ee82056f7538
Nessus-7.1.2-ubuntu1110_amd64.deb	5e69f44ba8e8671cff3a16dca97789e0
Nessus-7.1.2-ubuntu1110_i386.deb	5d3ec3be8ffcc9da3a3a7dbb407e9fe1
Nessus-7.1.2-ubuntu910_amd64.deb	865f40b773beca650d9726ac42c06201
Nessus-7.1.2-ubuntu910_i386.deb	69b25b85f48360fd8edb1501421e5b74
Nessus-7.1.2-Win32.msi	231c1501e6c6216d01149f845b9ef0e1
Nessus-7.1.2-x64.msi	5394b0906f479944587002a7c14e10ec

Nessus 7.1.3 Release Notes - 7/31/2018

> **Note:** If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New:

The following is a new feature included in Nessus 7.1.3:

- **Double the supported size of the Nessus Plugins Database** - The Nessus Engine was updated to support the handling of compiled plugin databases that exceed 2 GB in size. This prevents newer versions of the Nessus plugins that exceed the 2 GB size from resulting in a failure that would leave the scanner inoperable.

Bug fixes and Improvements:

- Fixed issue where Nessus Professional customers were unable to upgrade to Tenable Vulnerability Management when using a proxy
- Fixed upgrade banner at bottom of page that blocked scan results

File Names & MD5 Checksums

File	MD5
Nessus-7.1.3-amzn.x86_64.rpm	6c38db4326887d1721b72ba891ec5c37
Nessus-7.1.3-debian6_amd64.deb	b70245710b5654bd8c5e2bf521cbfef2
Nessus-7.1.3-debian6_i386.deb	d10d8344734d8325f9e752f87c0bbd1a
Nessus-7.1.3-es5.x86_64.rpm	630b494dc54825353c4a052993dd7848
Nessus-7.1.3-es5.i386.rpm	3cb0c1b5fd185e1c0cefe9cec5ab391b
Nessus-7.1.3-es6.x86_64.rpm	082fa352a3d44a0ef584a82e7aaaedd1
Nessus-7.1.3-es6.i386.rpm	03ed912406cf6f54813ffe54d89fe996
Nessus-7.1.3-es7.x86_64.rpm	e7526fb0a7d19b525efc885e8ce1c403
Nessus-7.1.3-fbsd10-amd64.txz	8114eef4f69296ad90a85356edd2e78f
Nessus-7.1.3-fc20.x86_64.rpm	ae36419325eb2a42b6e5b8747bd7a757
Nessus-7.1.3.dmg	eecb556e5456655836e99839b2a8ea73
Nessus-7.1.3-suse11.x86_64.rpm	6e98d78a0234851ded3604dd861427d4
Nessus-7.1.3-suse11.i586.rpm	40af64dbba38ee7f2331552dee299024
Nessus-7.1.3-suse12.x86_64.rpm	2ce616d525c2322a21e38386c6b57ec9
Nessus-7.1.3-ubuntu1110_amd64.deb	6037efdcec8f0559a1560da007bc98ef
Nessus-7.1.3-ubuntu1110_i386.deb	6e0e670481ad29e729b45a22cfc0d679

File	MD5
Nessus-7.1.3-ubuntu910_amd64.deb	6928ce48096178c221596d04f271c096
Nessus-7.1.3-ubuntu910_i386.deb	dc616069c1466c9a3226b8b680836f04
Nessus-7.1.3-Win32.msi	3e0350dae7902ffb6ef11bdf02547204
Nessus-7.1.3-x64.msi	260a79f20e05c24272f9572f103ac20c

Nessus 7.1.4 Release Notes - 12/19/2018

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes

- Updated openSSL patch level 1.0.2q to ensure latest security fixes are available

Nessus 7.1.5 Release Notes - 2019-08-08

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue with plugin size causing a significant impact on feed updates and scanning on Nessus Scanners.	N/A
Updated openSSL patch level 1.0.2s to ensure latest security fixes are available.	N/A

Nessus 7.2.0 Release Notes - 8/27/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: After you upgrade to Nessus 7.2.0, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New:

The following new feature is included in Nessus 7.2.0:

- Improved Scan Engine - The Nessus Scan Engine has been refactored to allow for greater scalability, to improve the codebase for greater maintainability, and to facilitate future improvements such as asynchronous I/O, load balancing, etc.

Bug fixes and Improvements:

- Fixed a bug where Nessusd -R is still running after upgrading to 7.2.0
- Fixed issue in Advanced settings where a user-created "new setting" is not persisted on the Advanced Settings page after returning

File Names & MD5 Checksums

File	MD5
Nessus-7.2.0-fbsd10-amd64.txz	7d4fe0be0bf7a2dffb9f510b2bf1046b
Nessus-7.2.0-debian6_i386.deb	bdb6d5f1b38a93c34cbcd36e6c1ff873
Nessus-7.2.0-debian6_amd64.deb	18fc0a4c2bd16432eb6a4332c2faf0e5
Nessus-7.2.0-es5.x86_64.rpm	4310f18c764f037597d0b80668b571bf
Nessus-7.2.0-es5.i386.rpm	94139519769f1787bc7128f341bebc76
Nessus-7.2.0-es6.x86_64.rpm	6ff4655a03474c8a9ddec07f08649a8a
Nessus-7.2.0-es6.i386.rpm	9c887f26b7c57d0c47ea0abcb0b95685

File	MD5
Nessus-7.2.0-amzn.x86_64.rpm	ec11863887c09937246366adf8e92a68
Nessus-7.2.0-suse11.x86_64.rpm	605906d599bc61bfbbac568397d4f495
Nessus-7.2.0-suse11.i586.rpm	9fe387c6543751db7c2476b7413d8546
Nessus-7.2.0-suse12.x86_64.rpm	cf0e39c22acd5c0ca776d3bc0ce7ebad
Nessus-7.2.0-ubuntu1110_amd64.deb	332111c61171f0bf37b9d7293f0844de
Nessus-7.2.0-ubuntu1110_i386.deb	0ce0fd56beb8b2c17e7b1f80f8700394
Nessus-7.2.0-fc20.x86_64.rpm	4d1e2ea56f0969246399e1e838a0984d
Nessus-7.2.0-es7.x86_64.rpm	851343bf731e30b84c6e837b211b8265
Nessus-7.2.0.dmg	cbbc33f41daa28b1c77f77a000d3db40
Nessus-7.2.0-Win32.msi	c9bc20e3b6e79f3609d0e0cff26d3aa9
Nessus-7.2.0-x64.msi	6b0fa2d3aa2a2d159e084942a7b17b77
nessus-updates-7.2.0.tar.gz	4c6b2d6d26d359675483881089709350

Nessus 7.2.1 Release Notes - 10/11/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: After you upgrade to Nessus 7.2.1, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New:

- Various documentation and template updates:
    - MobileIron Custom Port Support
    - Fixed credential failure with Lieberman integration
    - Added Huawei local checks to Credentialed Patch Audit
    - Updated PCI scan policy
    - Added PhotonOS to plugin family lists in policy templates

Bug Fixes and Improvements:

- Fixes to recent bugs that were found in the new scan engine released in Nessus 7.2

File Names & MD5 Checksums

File	MD5
Nessus-7.2.1-x64.msi	13261eb221b0305fc0097b2b85419172
Nessus-7.2.1-Win32.msi	bc9c3ce00306575d2d36ee77e787e62d
Nessus-7.2.1.dmg	1a993d2161953efc4933ac84a3a46157
Nessus-7.2.1-debian6_amd64.deb	b6c68a596f688950e037befde99326f2
Nessus-7.2.1-es5.x86_64.rpm	409a0b0dda87293b89ac67937479857f
Nessus-7.2.1-es6.x86_64.rpm	0f4c87ef1eeb8a894bc24668d0ce1871
Nessus-7.2.1-suse11.x86_64.rpm	45fc44aa8aa7609254266e8951425cab
Nessus-7.2.1-es7.x86_64.rpm	8699288c813ece3dfe9d2a6f951b49b4
Nessus-7.2.1-ubuntu1110_i386.deb	8b1250c4c03f7fb6156eba8945c519bb
Nessus-7.2.1-suse12.x86_64.rpm	70d6b81600c2c1fcdfca010ab7995bf8
nessus-updates-7.2.1.tar.gz	f8e5020a644a1261b2dccac532be5357
Nessus-7.2.1-amzn.x86_64.rpm	e0d73b6e234c8c058d57214635f906c0
Nessus-7.2.1-debian6_i386.deb	1ced95686afa6e1b91367fda661c75cb

File	MD5
Nessus-7.2.1-es6.i386.rpm	277121f7bff2095bd969b4e1e5f79c7f
Nessus-7.2.1-fc20.x86_64.rpm	aaf50b01b6745ac4f29be212c3acb97b
Nessus-7.2.1-suse11.i586.rpm	edc342b654b620e41e474ba4627b9a12
Nessus-7.2.1-es5.i386.rpm	73c15939d733fe5bcf9b23a813ecd504
Nessus-7.2.1-ubuntu1110_amd64.deb	1651afd3f8ceca439fb6f1d46e17b0cb
Nessus-7.2.1-fbsd10-amd64.txz	b7dd54d1b86a70262d97c3078f86f57f

Nessus 7.2.2 Release Notes - 11/08/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Do not install this version if you have already upgraded to Nessus 8. Please back up your system before installing a new version.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes and Improvements:

- Updated Nessus Manager to fix an issue with automatic software updates of linked Agents running the Agents 7.1.1 release.

Filenames & MD5 Checksums

For a full list of file names and checksums for this release, see the Tenable Downloads Page.

To get the MD5 and SHA256 checksums for a file, click **Checksum** in the **Details** column.

Nessus 7.2.3 Release Notes - 2019-08-08

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue with plugin size causing a significant impact on feed updates and scanning on Nessus Scanners.	N/A
Updated openSSL patch level 1.0.2s to ensure latest security fixes are available.	N/A

Nessus 8.0.0 Release Notes - 10/23/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

You can upgrade from Nessus 6.x or later to Nessus 8.0.0.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

What's New:

The following new features are included in Nessus 8.0:

- **Live Results:** When users enable Live Results on a scan, Nessus checks newly-released plugins against previously collected scan data without having to run a full new scan.

- **Vulnerability Snoozing/Inboxing:** Users can “snooze” a vulnerability for a period of time, allowing them to focus on the vulnerabilities they wish to handle now, while having the ones they want to see later reappear after the set time period.
- **Local Log Extraction:** Users can download local Nessus logs for troubleshooting from the Nessus user interface.
- **Vulnerability Grouping:** Users can group vulnerabilites together by application, plugin, etc. so that the list of scan results is truncated and shows related vulnerabilities together.

The following features are being added back into Nessus reports with Nessus 8.0:

- Re-enabled collapsibility and expandability of HTML report sections
- Re-added color-coded bullets to show severity of plugin vulnerabilities

Bug Fixes and Improvements:

- Fixed issue with report mismatch on port 53
- Changed the verbiage of "Licensed Hosts: None"
- Fixed issue in which UI becomes inaccessible due to scans being stuck in "processing" when attaching reports to emails
- Updated Nessus so that accounts that got locked and have only one user can be unlocked
- Fixed issue where Nessus Manager agent "platform" changes did not persist
- Restored support for printing scan results from browser's print function
- Fixed report export sorting
- Fixed issue where the expiration date changes when plugins are manually updated
- Fixed issue where error is displayed though proper scan name and target file was uploaded
- Fixed issue in advanced settings where duplicate settings can be created if default setting is renamed
- Fixed issue where plugin editor failed to correctly show all when that filter was enabled
- Fixed issue in which Nessus Manager delivers a diff update with incorrect checksum
- Fixed KMS helper build errors

File Names & MD5 Checksums

For a full list of file names and checksums for this release, see the Tenable Downloads Page.

To get the MD5 and SHA256 checksums for a file, click **Checksum** in the **Details** column.

Nessus 8.0.1 Release Notes - 11/01/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: After you upgrade Nessus, downgrading to a prior version of Nessus is not supported. Please back up your system first.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes:

- Updated Nessus Manager to fix an issue with automatic software updates of linked Agents running the Agents 7.1.1 release.
- Reinstated the 'nessusd -X' command, which provides the ability to export a list of available plugins.

File Names & MD5 Checksums:

For a full list of file names and checksums for this release, see the Tenable Downloads Page.

To get the MD5 and SHA256 checksums for a file, click **Checksum** in the **Details** column.

Nessus 8.1.0 Release Notes - 12/4/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.1.0.

New Features

The following are the new features included in the Nessus 8.1.0 Release:

- **Dynamic Scan Policies** – Often you may need to scan your client's environment for vulnerabilities with a specific type of behavior, for example, all vulnerabilities with a known exploit. In the past, with each plugin release, users would have to add each of these plugins to their policy manually. Now, using Dynamic Scan Policies, users can build a scan by creating a specific filter, e.g., all exploitable, and incorporating the filter into the scan policy. By using these filters with your scan policies, new plugins that match the filter are automatically added to the policy.

- **Revamped Advanced Settings Page** - Improved the Advanced Settings UI to allow for a more straightforward view of these advanced controls.

- **Remote Log Extraction** - Troubleshooting scans and agents can be a significant challenge. With the release of 8.0, we simplified this by allowing users to collect local logs directly from the UI. With this release, we are laying the foundation to also be able to request remote logs from managed scanners and agents.

  > **Note:** Scanners need to be running 8.1 or later and agents need to be running 7.2 or later.

- **Internationalized Dates** - Update the Nessus UI to use the international standard date notation, YYYY-MM-DD, where dates are shown.

- **Update to SSL Ciphers** - Use strong ciphers by default when negotiating SSL connections.

- **Non-credentialed scan optimization** - To decrease the time it takes to run scans, we have updated the logic for non-credentialed scans launched from Nessus to avoid running specific plugins that require credentials to work. Additionally, this significantly improves scan times for Host Discovery scans.

Bug Fixes

- Fixed issue with vulnerability found on port 8834

- Corrected issue where unlinked Agents counted towards license usage in Nessus Manager

- Fixed issue that prevented hosts that included an underscore in their name from being scanned
- Fixed issue that could cause the SecurityCenter scan status bar to read greater than 100%
- Fixed issue that caused a crash when scanner metrics were shut down
- Fixed issue on FreeBSD with scanning targets not on the local subnet
- Fixed issue with honoring the 'Scan IP addresses in a random order' setting
- Fixed issue with detecting IP address aliases on a network interface

Nessus 8.1.1 Release Notes - 12/19/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Any previous version of Tenable Nessus can upgrade directly to Tenable Nessus 8.1.1.

Bug Fixes

- Updated openSSL patch level 1.0.2q to ensure latest security fixes are available.
- Fixed a session timeout issue with Agent scan imports to Tenable Security Center that was causing '500 Internal Server Error' responses.
- Increased the plugin timeout maximum to allow Airwatch scans to complete.

2017 Tenable Nessus

Nessus 6.9.3 Release Notes - 1/4/2017

Nessus 6.10.0 Release Notes - 1/31/2017

Nessus 6.10.1 Release Notes - 2/3/2017

Nessus 6.10.2 Release Notes - 2/21/2017

Nessus 6.10.3 Release Notes - 3/14/2017

Nessus 6.10.4 Release Notes - 3/21/2017

Nessus 6.10.5 Release Notes - 4/11/2017

Nessus 6.10.6 Release Notes - 5/24/2017

Nessus 6.10.7 Release Notes - 5/31/2017

Nessus 6.10.8 Release Notes - 6/21/2017

Nessus 6.10.9 Release Notes - 7/14/2017

Nessus 6.11.0 Release Notes - 8/7/2017

Nessus 6.11.1 Release Notes - 8/14/2017

Nessus 6.11.2 Release Notes - 10/26/2017

Nessus 6.11.3 Release Notes - 12/5/2017

Nessus 7.0.0 Release Notes - 12/12/2017

Nessus 6.9.3 Release Notes - 1/4/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Implement an agent back off after receiving an error from a controller
- Fix XSS vulnerability in scanner allow unsafe characters in scan name (Security Advisory)
- Fix escape character display issue in dropdown

File Names & MD5 Checksums

File	MD5
nessus -6.9.3-amzn.x86_64.rpm	df816406de9e1f54317ac9d479accc0a
nessus -6.9.3-debian6_amd64.deb	43610259211b4434a90b5277d8c518c0
nessus -6.9.3-debian6_i386.deb	543de0316106181217cefc0022f04292
nessus -6.9.3.dmg	716a3421bdec5da03ca3336e18db2fe1
nessus -6.9.3-es5.i386.rpm	c3d8623aa1a3208fac8ad408e4869d53

File	MD5
nessus -6.9.3-es5.x86_64.rpm	5f5204a4a50b280c8685ae3ccf721320
nessus -6.9.3-es6.i386.rpm	6682f62923778a2c1a62d0f7b205b6b4
nessus -6.9.3-es6.x86_64.rpm	5828d9cf7e2f6158b4a1513af902b7ba
nessus -6.9.3-es7.x86_64.rpm	b5629e3e3e967ce50dbae40621dcbe8f
nessus -6.9.3-fbsd10-amd64.txz	be6b9bd872d3aeb1ddd6a76e424853b2
nessus -6.9.3-fc20.x86_64.rpm	6db1104a17b317251e39343d8585ff78
nessus -6.9.3-suse10.x86_64.rpm	584e3a069a01933f6fd6e506a6d3514b
nessus -6.9.3-suse11.i586.rpm	bcf9d21787be2c175a60a4373deb8f7a
nessus -6.9.3-suse11.x86_64.rpm	5dd47563a2fd04aa5d38fca33920310a
nessus -6.9.3-ubuntu1110_amd64.deb	81d7b3ddee42bc73e1c5e63f46713681
nessus -6.9.3-ubuntu1110_i386.deb	6932b836d2e1208ea2435867145c9efc
nessus -6.9.3-ubuntu910_amd64.deb	030ef832ec3a2d0d1dec9650b99ad535
nessus -6.9.3-ubuntu910_i386.deb	ae22838c39ceb7b7825d32e9c5330859
nessus -6.9.3-Win32.msi	859f18e80d22b492c4694c5337a10f28
nessus -6.9.3-x64.msi	b06d5e896e21a50b7ec37d4734a16234
nessusagent-6.9.3-amzn.x86_64.rpm	960bfbcdd3f0b0377bd8c6b8b2a73745
nessusagent-6.9.3-debian6_amd64.deb	819374199ce5e0fa3b276a427e0def47
nessusagent-6.9.3-debian6_i386.deb	a044560473b9eef28a8dfaa6d9fb3886
nessusagent-6.9.3.dmg	07b9a8fb4840974711b5338f2b6197ee
nessusagent-6.9.3-es5.i386.rpm	14e36b4a66bd585a6a67f95a29ac6c2e
nessusagent-6.9.3-es5.x86_64.rpm	8996bddaee5c43351ece502190ccd024
nessusagent-6.9.3-es6.i386.rpm	8eda34de9000329e9d9376fb87667243

File	MD5
nessusagent-6.9.3-es6.x86_64.rpm	2fc3e9f5cb1acff6ee137bd39173aba0
nessusagent-6.9.3-es7.x86_64.rpm	904f04f0852e9c4869e9efa68b0aaa2d
nessusagent-6.9.3-fc20.x86_64.rpm	a2c9da4b55a01161c1e7058f698579f9
nessusagent-6.9.3-ubuntu1110_amd64.deb	05951f104e09587f8268be979143a83e
nessusagent-6.9.3-ubuntu1110_i386.deb	8308d547ecdaa7b2f3cdc23ecedf0f58
nessusagent-6.9.3-ubuntu910_amd64.deb	423c0d828427f2504970f23773063a85
nessusagent-6.9.3-ubuntu910_i386.deb	48e7e66e9b41caea34ec27e37c13a442
nessusagent-6.9.3-Win32.msi	37371776b010aa23f6bce7229b26675f
nessusagent-6.9.3-x64.msi	7e38b7b8f9b9dbd16c5f4b601448def8

Nessus 6.10.0 Release Notes - 1/31/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features / Expanded Platform Support

- Tenable Vulnerability Management Offline Scanner
- Support for Nessus agents + managed scanners on SUSE 11/12

Bug Fixes and Improvements

- Update users to SHA-2 from SHA-1 certificates
- Update in-product references to cloud to "Tenable.io"
- 8835 to default port list
- Reduce default max size and files for agent logs
- New NASL compiler for faster plugins
- Nessus agents determine Windows password complexity
- Agents/managed scanners work when cert on manager changes

- Max TCP sessions in settings adhered to
- Allow nessusd.messages to be rotated daily
- Error 409 when trying to export scan diffs
- Remediations display duplicate results
- Email address containing + are sent reports successfully
- Plugin 19506 on Linux and OSX agents shows no in scan results
- Custom Windows host entries whitelist failing
- Nessus-service will not start nessusd with re-used PID
- Agents with same name, localhost or 127.0.0.01 displayed
- Prevent duplicate folder names
- Scan description is not properly formatted
- Hiding a large number of plugins causes all plugins to disappear
- API documentation issues with export
- JSON parse error

File Names & MD5 Checksums

File	MD5
nessus-6.10.0-amzn.x86_64.rpm	8a2793152b1535c655d00b961e7aa3ec
nessus-6.10.0-debian6_amd64.deb	4e64f847bd8cc983d0ac8cafd363127e
nessus-6.10.0-debian6_i386.deb	8e5ac94ef0f714dfd6948784f3f1f05e
nessus-6.10.0.dmg	173436ed485533adae39402ad270bbf6
nessus-6.10.0-es5.i386.rpm	28fc5355a967ed9e8d58a21745d89be9
nessus-6.10.0-es5.x86_64.rpm	8d1decd8c867052a4674e0739ceef015
nessus-6.10.0-es6.i386.rpm	0ac83557b56b05cfdf0e44e4012eab52
nessus-6.10.0-es6.x86_64.rpm	74407dc649cc4fd1a62e748b050c37e4

File	MD5
nessus-6.10.0-es7.x86_64.rpm	9a1943276ba5965519b484a18f2417d3
nessus-6.10.0-fbsd10-amd64.txz	d7c989bafe697bdbcecd3ecf87171715
nessus-6.10.0-fc20.x86_64.rpm	f7149ed4d683a0f9220b01b62e4798b0
nessus-6.10.0-suse11.i586.rpm	3fa7b049f85455ae4230834c76b792cd
nessus-6.10.0-suse11.x86_64.rpm	afbd93a271e4576bb818d811f4e25642
nessus-6.10.0-suse12.x86_64.rpm	6bd1c92ce8c87416692d9d6054f42926
nessus-6.10.0-ubuntu1110_amd64.deb	8cdf5c16e3ae0a3857471c04f88d1f43
nessus-6.10.0-ubuntu1110_i386.deb	fc28b8fef2715d9c0c36456a3cf9fd2b
nessus-6.10.0-ubuntu910_amd64.deb	a413f53ea57c113b7671d7ea25f63f07
nessus-6.10.0-ubuntu910_i386.deb	22b969ef9b962dfafb18373b6bab65d6
nessus-6.10.0-Win32.msi	a612c70de7220d8aa2da34ee72126422
nessus-6.10.0-x64.msi	4cd196a55d385916d6f717e9df0144dd
nessusagent-6.10.0-amzn.x86_64.rpm	73d8067f2d1d8a5991176b0cec13384a
nessusagent-6.10.0-debian6_amd64.deb	99a31403f961ff5b9ec36d0522648944
nessusagent-6.10.0-debian6_i386.deb	02a95b230a93119a1efa479c2bc4a33f
nessusagent-6.10.0.dmg	53715cbdd50ca3f25bb6703df32a1399
nessusagent-6.10.0-es5.i386.rpm	a882bb0c3975e362066025e4e3f09d73
nessusagent-6.10.0-es5.x86_64.rpm	40b3920a64e23427cb173a53ac62dec0
nessusagent-6.10.0-es6.i386.rpm	747c4457e5ab27c0c3d66cb1507b1d06
nessusagent-6.10.0-es6.x86_64.rpm	55156118bd69410ab64a9eb4caebc2b4
nessusagent-6.10.0-es7.x86_64.rpm	f305fbb0b2e046bb78258dce81436a58
nessusagent-6.10.0-fc20.x86_64.rpm	0ef31e8d25373852453c3ef8755854d4

File	MD5
nessusagent-6.10.0-suse11.i586.rpm	0663b1e511a9ec82081c4a66c5e0addf
nessusagent-6.10.0-suse11.x86_64.rpm	35184fcfc6fd5a31aa659a319523e4bf
nessusagent-6.10.0-suse12.x86_64.rpm	dca8c27d98ae56abaf723d5e43dfc139
nessusagent-6.10.0-ubuntu1110_amd64.deb	cc39c5281f6a4dede03773bddd4a6f41
nessusagent-6.10.0-ubuntu1110_i386.deb	1950912dd34d15b768f8826fafde9de9
nessusagent-6.10.0-ubuntu910_amd64.deb	b0a6b162e1c974fd8408bec0b1661d35
nessusagent-6.10.0-ubuntu910_i386.deb	79aa896f6b1c3c1cb19ca25fba84dc13
nessusagent-6.10.0-Win32.msi	a1c07a91e39b679adabbf327ff50ecc8
nessusagent-6.10.0-x64.msi	f6aaa1ca067a867ac6d010aabec9eb99
nessus-debug-6.10.0_Win32.tar.gz	c59b1bfe49a04b87c6d572f4ba601419
nessus-debug-6.10.0_Win32_uNessus.tar.gz	b34d2bd47abe1e235d8e671f16fdaf10
nessus-debug-6.10.0_x64.tar.gz	a3d4a411552d0c45f8e5718428342343
nessus-debug-6.10.0_x64_uNessus.tar.gz	a796c5ec6aa6e39e0f5de03e4189164c

Nessus 6.10.1 Release Notes - 2/3/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- When linking Nessus to Tenable Vulnerability Management using the activation wizard, the scanner fails to link properly, even though it appears to be successful.

File Names & MD5 Checksums

File	MD5
nessus-6.10.1-amzn.x86_64.rpm	2e4350e8d137987cd20341eca1305563
nessus-6.10.1-debian6_amd64.deb	064b16cc19d2ae354283502b63e25271

File	MD5
nessus-6.10.1-debian6_i386.deb	7b648dca891bc5a9219c3fc2e44b0743
nessus-6.10.1.dmg	4c0eb75938e948e825ce36c55e5752e2
nessus-6.10.1-es5.i386.rpm	1b367e6f6a84d6251667b2ef53802b06
nessus-6.10.1-es5.x86_64.rpm	4347530afa6ac18681f62a493fe2505b
nessus-6.10.1-es6.i386.rpm	03647e6349f2ab6aaa20332b7b3684c4
nessus-6.10.1-es6.x86_64.rpm	2a874d4b21455dbee31fe6ab7be5f44e
nessus-6.10.1-es7.x86_64.rpm	f47cfff32beefda2c3ddeed84cd9c1fe
nessus-6.10.1-fbsd10-amd64.txz	8a02d522a6162a9f2a023a4a1e8f343c
nessus-6.10.1-fc20.x86_64.rpm	9ea15e55e57021840bc13ac208772e72
nessus-6.10.1-suse11.i586.rpm	fd59021d9daa4e82f53f7d17fe052af9
nessus-6.10.1-suse11.x86_64.rpm	fe0725e85ac7c243b87ea3345eb08fa2
nessus-6.10.1-suse12.x86_64.rpm	7970ba179adfeebf8f1d53c90dc1dd0c
nessus-6.10.1-ubuntu1110_amd64.deb	5f77d21aa167aac1ee5bf821cfc4e4f1
nessus-6.10.1-ubuntu1110_i386.deb	aafaff9a0c4dc76afefede83cb2f6a22
nessus-6.10.1-ubuntu910_amd64.deb	761e88041c41eebca26839f451670af7
nessus-6.10.1-ubuntu910_i386.deb	343cde2564c0af72991b96b3bfc073ff
nessus-6.10.1-Win32.msi	44ebad5cd0dec114a7075cb94dd62b27
nessus-6.10.1-x64.msi	a86ed8ddbf0dcd1df8817313a7cdcc5e
nessusagent-6.10.1-amzn.x86_64.rpm	0495ee2d60028cedb99e86c69248699a
nessusagent-6.10.1-debian6_amd64.deb	94bbc9a3b0fe75a7244c566dfef83811
nessusagent-6.10.1-debian6_i386.deb	142589cb5051494c97590a91f7710a27
nessusagent-6.10.1.dmg	ac1c86a8451a63748158cbb0b235d0e8

File	MD5
nessusagent-6.10.1-es5.i386.rpm	531289467ec46db6eb15480c8928eb79
nessusagent-6.10.1-es5.x86_64.rpm	a88f3f06ad1a0f952c1349e9fc22d483
nessusagent-6.10.1-es6.i386.rpm	51931f6047dedfe178fcb81e0be05ea6
nessusagent-6.10.1-es6.x86_64.rpm	1730cda5bf75c9392d65f75e85aee7cf
nessusagent-6.10.1-es7.x86_64.rpm	f180f6268c13aef55bfa642300247b42
nessusagent-6.10.1-fc20.x86_64.rpm	fff8f1cc01c1278975705e032953fdb5
nessusagent-6.10.1-suse11.i586.rpm	596765bbd6ef74db5b91c5463012c405
nessusagent-6.10.1-suse11.x86_64.rpm	467fe0ce4008cf5216d77ce25ff0a211
nessusagent-6.10.1-suse12.x86_64.rpm	c8ac73c178cb52d94ae32b1090d8ac01
nessusagent-6.10.1-ubuntu1110_amd64.deb	f99f825987a9b90eb328f406f8fcffb2
nessusagent-6.10.1-ubuntu1110_i386.deb	112d7a998c660031f788edb5d82d6c25
nessusagent-6.10.1-ubuntu910_amd64.deb	496742927e5452f3bb646e6374654848
nessusagent-6.10.1-ubuntu910_i386.deb	1bdd18e843202b09258aa83b7a9c4c54
nessusagent-6.10.1-Win32.msi	9c3d253efe4330b65b0706b2b1feac23
nessusagent-6.10.1-x64.msi	e24149c935f5c0a6f0ada6ade8c9fbf6

Nessus 6.10.2 Release Notes - 2/21/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix authenticated file upload vulnerability on Windows
- Prevent truncation of plugin info on HTML reports
- Plugin 91990 re-added to malware policy
- Remove extra commas from imported text file targets list

- Enable Host Tagging option for managed scanners only
- Fix empty page display on old version of Firefox

File Names & MD5 Checksums

File	MD5
nessus-6.10.2-amzn.x86_64.rpm	c1226ab037e6b6373156fbef1a5e535c
nessus-6.10.2-debian6_amd64.deb	6410eb34156de8873e07e1207df55601
nessus-6.10.2-debian6_i386.deb	62212ee9e15ec1e383e0dad4b7816274
nessus-6.10.2.dmg	d57d2d1446b224f03b658ad32004de11
nessus-6.10.2-es5.i386.rpm	de6a52ec821d98d839386d9bfc5db822
nessus-6.10.2-es5.x86_64.rpm	2a7ee85e5f7078b5a2fd4724056c1088
nessus-6.10.2-es6.i386.rpm	6da95ec6b47423a9088b22953bf4e5c9
nessus-6.10.2-es6.x86_64.rpm	0b482bc94608df88ce8f3c7eecf777d8
nessus-6.10.2-es7.x86_64.rpm	6488cdb939b14d865390eeec58c062a3
nessus-6.10.2-fbsd10-amd64.txz	18b30d1ec21586d29154b381ad963401
nessus-6.10.2-fc20.x86_64.rpm	6d283bb4ddb150aacb757acddbe368ea
nessus-6.10.2-suse11.i586.rpm	4484acc795d9d79d879c0597f7ddea37
nessus-6.10.2-suse11.x86_64.rpm	e58d7f4f5d6bb3f0c12741d157be32bb
nessus-6.10.2-suse12.x86_64.rpm	90df29f366a981673cf737d394bbda45
nessus-6.10.2-ubuntu1110_amd64.deb	692577b217fc618e402cebdbfc980c9b
nessus-6.10.2-ubuntu1110_i386.deb	999a4925bcd0d518a71b4733732c91cf
nessus-6.10.2-ubuntu910_amd64.deb	6e038d45f4ab71099de8194743c5646b
nessus-6.10.2-ubuntu910_i386.deb	b0f558de81fa8403ce0e74eaa56aea36
nessus-6.10.2-Win32.msi	92d69f9641906420b05f5c81aacb85a8
nessus-6.10.2-x64.msi	b40506933f3df33f090ea45c89093060

File	MD5
nessusagent-6.10.2-amzn.x86_64.rpm	dd91e1e877179bfb13198f19e97989e2
nessusagent-6.10.2-debian6_amd64.deb	07003fda6f25ac3cc3b444d8f0b70f86
nessusagent-6.10.2-debian6_i386.deb	352026c33003a5634dcc037d05efe956
nessusagent-6.10.2.dmg	5e82bf6215caa1a6683d6de1f777af4c
nessusagent-6.10.2-es5.i386.rpm	2cdb076570512c561cf172b43f90dfe9
nessusagent-6.10.2-es5.x86_64.rpm	5a8854923bd0c4623363b192045b9bb7
nessusagent-6.10.2-es6.i386.rpm	b71a8e7aa47a1065cd08bc77ef06aadc
nessusagent-6.10.2-es6.x86_64.rpm	61866bc0b65cba91dbf9adfdf318fc88
nessusagent-6.10.2-es7.x86_64.rpm	0a42d5838aac2e468663463e1133a6e3
nessusagent-6.10.2-fc20.x86_64.rpm	c1995cd2e7276155ac34ca70771404b5
nessusagent-6.10.2-suse11.i586.rpm	fbd14f900060fc45fd3f3ddd5bdbc3bf
nessusagent-6.10.2-suse11.x86_64.rpm	c5354ac8a5b728eb5d7a4abdb3831b93
nessusagent-6.10.2-suse12.x86_64.rpm	11f8bb500ff15e770d9420b39025482e
nessusagent-6.10.2-ubuntu1110_amd64.deb	9b5b955d4b14d85d272202ac85e82264
nessusagent-6.10.2-ubuntu1110_i386.deb	70496b39879ae9e5f1c9a708f8cb65a9
nessusagent-6.10.2-ubuntu910_amd64.deb	b4108bf59e2b5e053a2898b84e5a2484
nessusagent-6.10.2-ubuntu910_i386.deb	5428ab4e8f4c4ffb4c26175427207a8b
nessusagent-6.10.2-Win32.msi	73d096bd4f2495473180bbe161bf8903
nessusagent-6.10.2-x64.msi	95cfa585912c863252c34df98fd9c999

Nessus 6.10.3 Release Notes - 3/14/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Update expired MacOS Developer certificate on build server
- Include Yara to plugin 91990
- Remove truncation of custom PDF report grouped by plugin

File Names & MD5 Checksums

File	MD5
nessus-6.10.3-amzn.x86_64.rpm	688a8134ba904f89445833d94afe424a
nessus-6.10.3-debian6_amd64.deb	ab926dd6257a04778eb9fafe43eb559d
nessus-6.10.3-debian6_i386.deb	ac3d6ad37244d6ff0f0422e81e1c8cd1
nessus-6.10.3.dmg	a588f804ed7716c8c9f9b6b7fa76544d
nessus-6.10.3-es5.i386.rpm	424d955cad22cc208acacc4529b8fda2
nessus-6.10.3-es5.x86_64.rpm	9962038005842e6970471975917b28a8
nessus-6.10.3-es6.i386.rpm	78955c913f8d16fef3554a9e839daa44
nessus-6.10.3-es6.x86_64.rpm	4045ea52cee38f053494a37f03ef0795
nessus-6.10.3-es7.x86_64.rpm	1f3f18207db6332ace911cf83d5594ed
nessus-6.10.3-fbsd10-amd64.txz	72efdc15a5e28487fe6c93b8a1dd1189
nessus-6.10.3-fc20.x86_64.rpm	e52ac3e817e12c2482a93aa48ea98a1c
nessus-6.10.3-suse11.i586.rpm	9bb9ff09eea64846025f83d3738c9fda
nessus-6.10.3-suse11.x86_64.rpm	67318b82f79fc4102f38b80c4c444a0c
nessus-6.10.3-suse12.x86_64.rpm	50bd3429fdf06d9e07a45f8bd0e85a54
nessus-6.10.3-ubuntu1110_amd64.deb	d316abae087bc8d3aea34d5413aa5780
nessus-6.10.3-ubuntu1110_i386.deb	e48268d6107b6bf2e0911848d2d891a0
nessus-6.10.3-ubuntu910_amd64.deb	d4b87af84d211ac8f59a0762e4afb955
nessus-6.10.3-ubuntu910_i386.deb	448eeec28229b172dc21b133d329ba39
nessus-6.10.3-Win32.msi	191d11a1d61936c942a73abd7e6ff1d5

File	MD5
nessus-6.10.3-x64.msi	c64181608011546f2353ba8b24be823e
nessusagent-6.10.3-amzn.x86_64.rpm	50cd9be9a02d7ceb4fa1e89cbe374064
nessusagent-6.10.3-debian6_amd64.deb	219a14bb3451a53125df14c828e5c5a0
nessusagent-6.10.3-debian6_i386.deb	692369bd268ae907b29047328e612780
nessusagent-6.10.3.dmg	e5de4ab45e0cb04d07d5266bee629c71
nessusagent-6.10.3-es5.i386.rpm	5c8304201583df442494615987791be4
nessusagent-6.10.3-es5.x86_64.rpm	f33e777f345dbc1fbc7d075b5d73b90f
nessusagent-6.10.3-es6.i386.rpm	659abf08182d07d6296588f87c6d97d9
nessusagent-6.10.3-es6.x86_64.rpm	f3651114d45d0fc129bfc5e3215cfd9e
nessusagent-6.10.3-es7.x86_64.rpm	e62ee0cefc3ee1c80fa43ca2f933c85d
nessusagent-6.10.3-fc20.x86_64.rpm	c649a2c290877e5b5859c751168eb2eb
nessusagent-6.10.3-suse11.i586.rpm	5ae7aaff4a4069ec44d3bdd32ad5bbef
nessusagent-6.10.3-suse11.x86_64.rpm	c41fbf7bf07726001c78f97b2ff42318
nessusagent-6.10.3-suse12.x86_64.rpm	e2ddcc0c2fa4b6d2a71a164001a4fa7a
nessusagent-6.10.3-ubuntu1110_amd64.deb	7320b6e53fda8e006867d829514e3b12
nessusagent-6.10.3-ubuntu1110_i386.deb	fd7731015e89cad67d950fb6c92590d4
nessusagent-6.10.3-ubuntu910_amd64.deb	19f331aa18c845855a3f8e8119b11a6e
nessusagent-6.10.3-ubuntu910_i386.deb	ce25024bbecc7b8d4d884370818ce2fd
nessusagent-6.10.3-Win32.msi	386cb125d8d2d20600a605bdb6e01004
nessusagent-6.10.3-x64.msi	04685304445c27e446d582751b47ed6b

Nessus 6.10.4 Release Notes - 3/21/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix resolving a plugin causing a scan to hang in certain conditions

File Names & MD5 Checksums

File	MD5
nessus-6.10.4-amzn.x86_64.rpm	71103d3a40fd6aad058ebcd5f926686a
nessus-6.10.4-debian6_amd64.deb	3f1be5716477aac7ebe93ecb1dcbd5f7
nessus-6.10.4-debian6_i386.deb	2379f399c48254a8bd8a995383a86747
nessus-6.10.4.dmg	d91f76a047ae4db01f71e8540582f6c0
nessus-6.10.4-es5.i386.rpm	570c36389d2645b939f9a5097ab37ce8
nessus-6.10.4-es5.x86_64.rpm	df393b1272aaca0d6a2efcef6c320f1c
nessus-6.10.4-es6.i386.rpm	393d0331f8502ae6543f0873f1c12027
nessus-6.10.4-es6.x86_64.rpm	427226def174725a39557d8bc663d602
nessus-6.10.4-es7.x86_64.rpm	233229eae796020f28e39212f671fe6e
nessus-6.10.4-fbsd10-amd64.txz	890f1ac7eb399bbce6287e88c00251cc
nessus-6.10.4-fc20.x86_64.rpm	5c889cfb9bf34343e002bdd09e79ab5f
nessus-6.10.4-suse11.i586.rpm	e128d09b5942adcae5f4476dbb224c17
nessus-6.10.4-suse11.x86_64.rpm	c68e6f16d3e94d6e60c130314a8e3356
nessus-6.10.4-suse12.x86_64.rpm	7aea8e35b6194ded946367f0c7b38e03
nessus-6.10.4-ubuntu1110_amd64.deb	d708ca659ee8347dedb06c6579177e1e
nessus-6.10.4-ubuntu1110_i386.deb	940dca282dd5982780f078f8fc47d32f
nessus-6.10.4-ubuntu910_amd64.deb	eaf0b2fe4cbf5763a1393604c860fc83
nessus-6.10.4-ubuntu910_i386.deb	71fdc74f7be4a07a91ad486091610c31
nessus-6.10.4-Win32.msi	1a8a96abec7cfe6a5c1e714e76b1df90
nessus-6.10.4-x64.msi	335c133511f327669f586e3baefc8d0d
nessusagent-6.10.4-amzn.x86_64.rpm	0c838b9580f245a49bb2582f55e204d8

File	MD5
nessusagent-6.10.4-debian6_amd64.deb	ff4ab7aa7ba155c4c0aae7ef50b03dc3
nessusagent-6.10.4-debian6_i386.deb	a775428ebabd852f371a2c3d0b488b16
nessusagent-6.10.4.dmg	7ba1bdcb5c802d6547d7c758828dd2c1
nessusagent-6.10.4-es5.i386.rpm	ee0bcbedd00cbed71cd2e11ebfff1df4
nessusagent-6.10.4-es5.x86_64.rpm	75c19d4a440bab3965534ed942cf0116
nessusagent-6.10.4-es6.i386.rpm	37fc225409b888782ac9e92c848a9ce6
nessusagent-6.10.4-es6.x86_64.rpm	7b1a31636b1a343f375bb8200bc60d25
nessusagent-6.10.4-es7.x86_64.rpm	45339d3dda09e13983cf81258fc23114
nessusagent-6.10.4-fc20.x86_64.rpm	28edb3f4876e87a612315592ca2e6dc9
nessusagent-6.10.4-suse11.i586.rpm	1731b75181b21d796275affde61130f5
nessusagent-6.10.4-suse11.x86_64.rpm	f61c0f1f3eb6639765135a45879f3bb6
nessusagent-6.10.4-suse12.x86_64.rpm	98e811fdbeee53564d867be11613ba7c
nessusagent-6.10.4-ubuntu1110_amd64.deb	52e198ea0c9560cdbaaef80529d0b63f
nessusagent-6.10.4-ubuntu1110_i386.deb	ecd43a9c3c3450c4825328424cf64da4
nessusagent-6.10.4-ubuntu910_amd64.deb	f217fc76355d0bce71a3d678459838f1
nessusagent-6.10.4-ubuntu910_i386.deb	718171b44adbe6ea472e55852cfe1e9b
nessusagent-6.10.4-Win32.msi	8d8429489a4293ce0488801f6eca15d8
nessusagent-6.10.4-x64.msi	2350b620d8170d4b227ef814bde904d0

Nessus 6.10.5 Release Notes - 4/11/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Improve process to upload custom certificates for plugin 51192
- Fix for scanning virtual hosts behind a load balancer
- Allow AWS pre-auth scanner to register via proxy
- Fix for a database bug after plugin updates

File Names & MD5 Checksums

File	MD5
nessus-6.10.5-amzn.x86_64.rpm	291140cff4a29fd9372cae266c33bcd5
nessus-6.10.5-debian6_amd64.deb	bbf8a19c88b3dae08ead8be73e9c494e
nessus-6.10.5-debian6_i386.deb	3628b0fe3f1447415f8c6a186b3dda7f
nessus-6.10.5.dmg	31a889e8b6ebdc85fa5c1f09719edc27
nessus-6.10.5-es5.i386.rpm	9b9272c9766495f7a69762e93b32da57
nessus-6.10.5-es5.x86_64.rpm	272649f69fa9e9564d8db9c952d58085
nessus-6.10.5-es6.i386.rpm	96b80a59707745d9bfd42e952bcc875e
nessus-6.10.5-es6.x86_64.rpm	eb8b39056ce3524f273c6572b7f4627a
nessus-6.10.5-es7.x86_64.rpm	83ae1a421826bf797b59672a37fe0357
nessus-6.10.5-fbsd10-amd64.txz	62489b89118477f57128e5deebbc856e
nessus-6.10.5-fc20.x86_64.rpm	a2cc1de7c78efe7f1c2034f7ceb20852
nessus-6.10.5-suse11.i586.rpm	2117fcdfc519d6f354627b173a5000f6
nessus-6.10.5-suse11.x86_64.rpm	8d9fb84af6449a789ac09e37658fb71f
nessus-6.10.5-suse12.x86_64.rpm	348ab48a0b9ef64a54eddd1bf1ef6e75
nessus-6.10.5-ubuntu1110_amd64.deb	86c422ea6cd4f5e09894379b7c1c82b7
nessus-6.10.5-ubuntu1110_i386.deb	1e50843a5377ce1d1f8ad0e62688c7c2
nessus-6.10.5-ubuntu910_amd64.deb	7ffd8272bd3dce51ccb75e9a6a8ad1ab
nessus-6.10.5-ubuntu910_i386.deb	dc5e4e8a1025fb33b648418ee87f4651

File	MD5
nessus-6.10.5-Win32.msi	8abcc3b8945e59059b0e2f5e31de158c
nessus-6.10.5-x64.msi	4ac761a022e0eec965a1e18a46383360
nessusagent-6.10.5-amzn.x86_64.rpm	48d562c25d7548e818584cad13a20ad3
nessusagent-6.10.5-debian6_amd64.deb	3bf4666797086133c532f0afe0a5921f
nessusagent-6.10.5-debian6_i386.deb	afa71350d7272880c13d03ef829665ab
nessusagent-6.10.5.dmg	8ce94f120297248f82a329b37ae05566
nessusagent-6.10.5-es5.i386.rpm	673ee9b3717ae759b9b9520609071add
nessusagent-6.10.5-es5.x86_64.rpm	ae0234e38af680ce5cde8a8082b496d3
nessusagent-6.10.5-es6.i386.rpm	c34b600e23dbc63e710204933cafc26a
nessusagent-6.10.5-es6.x86_64.rpm	25afd5f9b670c3d327ef10a0939fbf40
nessusagent-6.10.5-es7.x86_64.rpm	eb33547910fb4f70aadf4f414a753610
nessusagent-6.10.5-fc20.x86_64.rpm	5c1c84641c14af318a955022c3eb39ec
nessusagent-6.10.5-suse11.i586.rpm	bb8023f4f99d64e85d5c2ee36f601478
nessusagent-6.10.5-suse11.x86_64.rpm	60ffdba918eb3cd3d09d2c99843d90ab
nessusagent-6.10.5-suse12.x86_64.rpm	67543a54ac1b30ca0211ff3bdd56fadd
nessusagent-6.10.5-ubuntu1110_amd64.deb	4c72583c85c982ccd714809a8276bc5b
nessusagent-6.10.5-ubuntu1110_i386.deb	69085f304e8dfadfa3f70593cedb79f0
nessusagent-6.10.5-ubuntu910_amd64.deb	57a65cf99f1877de3cfa37aa9a15d05a
nessusagent-6.10.5-ubuntu910_i386.deb	274fc3cadc5e36b029aa99ca4484a3b8
nessusagent-6.10.5-Win32.msi	58e2c1d09354b27b2231ac059d1be118
nessusagent-6.10.5-x64.msi	c1102cff319dfcf683be959942c56d8e

Nessus 6.10.6 Release Notes - 5/24/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Added policy for WannaCry
- Added policy for Intel AMT Vuln
- Added ability to add custom URL to CyberArk credentials
- Fix timezones in reports
- Fix a client issue where plugins no longer update
- Fix to honor port ranges

File Names & MD5 Checksums

File	MD5
nessus-6.10.6-amzn.x86_64.rpm	84196d591e4c1bf529a9aa07a17f227d
nessus-6.10.6-debian6_amd64.deb	18e367aadb1488cfcc1a189e6a42702a
nessus-6.10.6-debian6_i386.deb	2b33d8aa68b39eefbea4f9b72aae48db
nessus-6.10.6.dmg	9df6e0629fb994afe3dc36a1df81ef37
nessus-6.10.6-es5.i386.rpm	e2a043949af6d23601bca5dea60bb1c7
nessus-6.10.6-es5.x86_64.rpm	8e4efcf3d6b9ecd74fbe253c09e0a30a
nessus-6.10.6-es6.i386.rpm	0b803503a230968de0d2d2fff91013a2
nessus-6.10.6-es6.x86_64.rpm	8df625cdbff3dfc3d1bf5d7342e953ea
nessus-6.10.6-es7.x86_64.rpm	e9b2e996fe076af69e9f9cf7579ba691
nessus-6.10.6-fbsd10-amd64.txz	52164674a6e0be33892af1411929463d
nessus-6.10.6-fc20.x86_64.rpm	d6e3ecc434e19329d10fac1d37b26b29
nessus-6.10.6-suse11.i586.rpm	e45c83a7f2fa603c8b3002850260f1e5
nessus-6.10.6-suse11.x86_64.rpm	ea47c057b09e59ede24cb855c60895e9

File	MD5
nessus-6.10.6-suse12.x86_64.rpm	8384e36e78a307f4752cca5b4df93242
nessus-6.10.6-ubuntu1110_amd64.deb	ae5d977635c60fc9896cc7b31bf96850
nessus-6.10.6-ubuntu1110_i386.deb	e18dcb8e62ea23da608df10994279b60
nessus-6.10.6-ubuntu910_amd64.deb	ef2249f428a9b4aee70488d406e63562
nessus-6.10.6-ubuntu910_i386.deb	06277ed0c58bae6640060964ed598194
nessus-6.10.6-Win32.msi	aa6890663dfc46535257474459c8cc68
nessus-6.10.6-x64.msi	949c08a0dc555f82a7b209b211f147e4
nessusagent-6.10.6-amzn.x86_64.rpm	c6a84765d070a8a355804fec653fd8a7
nessusagent-6.10.6-debian6_amd64.deb	440096986d01280b10fb92e71d35babd
nessusagent-6.10.6-debian6_i386.deb	dbfae4825074da66b991319ae7599217
nessusagent-6.10.6.dmg	13957a4ac33900329737c54acae8e366
nessusagent-6.10.6-es5.i386.rpm	488ef39491bbaf68ea624f3f517dab3b
nessusagent-6.10.6-es5.x86_64.rpm	e77796c4d2709230a7ded90de8598184
nessusagent-6.10.6-es6.i386.rpm	6482cb322373788f30e5a3565d2fafd9
nessusagent-6.10.6-es6.x86_64.rpm	e5e870db2c524d173444599626982a7d
nessusagent-6.10.6-es7.x86_64.rpm	160b629878fe5b5680e62689c7957aa3
nessusagent-6.10.6-fc20.x86_64.rpm	6fb0089e743c38f01902564d289eb0c2
nessusagent-6.10.6-suse11.i586.rpm	1322da6cc0b0ed86b20ee6976afece69
nessusagent-6.10.6-suse11.x86_64.rpm	6a0ffe212439da9fec1da425fba6103b
nessusagent-6.10.6-suse12.x86_64.rpm	241c6d94f9813ba6f2aacdebe9e2dfa3
nessusagent-6.10.6-ubuntu1110_amd64.deb	10137a2fc9465ae1fe17b3ce48981ff5
nessusagent-6.10.6-ubuntu1110_i386.deb	e0bc2ef8a6391c027999621177a35be8

File	MD5
nessusagent-6.10.6-ubuntu910_amd64.deb	8ccc43fd857289b4f3cb0f3e6f6dbbad
nessusagent-6.10.6-ubuntu910_i386.deb	88cc37b7d5c9657faf191da0a9a0a6fd
nessusagent-6.10.6-Win32.msi	a4864e28cdb3229dd22c4e8aeca011f3
nessusagent-6.10.6-x64.msi	cbfecff75ab9a82db62721f09167e1a0

Nessus 6.10.7 Release Notes - 5/31/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Added policy to detect disclosed Shadow Broker vulnerabilities
- Fix to prevent folders from being created unintentionally

File Names & MD5 Checksums

File	MD5
nessus-6.10.7-amzn.x86_64.rpm	b608207dd73eaca401616bb2e7a972d5
nessus-6.10.7-debian6_amd64.deb	3ea000e3d744aaea026ec5a4b0122ff5
nessus-6.10.7-debian6_i386.deb	b9910a5d229c8f9c7b0e237466f08337
nessus-6.10.7.dmg	e7b7c1b8b5a4044ecad925b3480bb750
nessus-6.10.7-es5.i386.rpm	d7d37209365b73304b1a4231a46bedbb
nessus-6.10.7-es5.x86_64.rpm	3d440c9bfaec39920c9cee760317161e
nessus-6.10.7-es6.i386.rpm	5161e8a41993a7691c093a5e13b3480b
nessus-6.10.7-es6.x86_64.rpm	24c1e38c4224a02782d8ed0b8800fd65
nessus-6.10.7-es7.x86_64.rpm	f5e816b49b16ecefa37cbf6fda9aa7a5
nessus-6.10.7-fbsd10-amd64.txz	172e52eb60ca7d2c8eaece2bd5adc8d9
nessus-6.10.7-fc20.x86_64.rpm	0724709ea9b5522d3fab8fc20f5f0fef

File	MD5
nessus-6.10.7-suse11.i586.rpm	7241826eb57b6295d92bb016845c5e50
nessus-6.10.7-suse11.x86_64.rpm	cf18f47add8d861f326e22f4d1539f83
nessus-6.10.7-suse12.x86_64.rpm	1c6cb94d4fbf1741b18985f37f7c23f0
nessus-6.10.7-ubuntu1110_amd64.deb	cea5f308f952fcadb6ebe157109bb036
nessus-6.10.7-ubuntu1110_i386.deb	a114777ab3798da9980f4af14176eba7
nessus-6.10.7-ubuntu910_amd64.deb	c348d5e795c68d5f6e713c70d94ded23
nessus-6.10.7-ubuntu910_i386.deb	ddb1fca94b60f34bbdc90f4ef97f232b
nessus-6.10.7-Win32.msi	41c922a7387d4cd8b20090ff669db3d8
nessus-6.10.7-x64.msi	9d0beb5d2b3b351279b13917208c1f44
nessusagent-6.10.7-amzn.x86_64.rpm	350c1b60d2ccc75dc867e7725d5b41ac
nessusagent-6.10.7-debian6_amd64.deb	7bac430cc411e241197c5031fa775cb8
nessusagent-6.10.7-debian6_i386.deb	98e52deab2c92608bd3e6b6e5dd64844
nessusagent-6.10.7.dmg	6e46d6b315d19d9f26964003ec319e0d
nessusagent-6.10.7-es5.i386.rpm	5be01c1da4bda3fbe46b33747c3c56ef
nessusagent-6.10.7-es5.x86_64.rpm	ec4ebba5d224f0ca51868bafeb590ab9
nessusagent-6.10.7-es6.i386.rpm	667a8ffdd3811a9ee18c42c61179ebea
nessusagent-6.10.7-es6.x86_64.rpm	cd40892e9c7e4543ba1c5b487a9da220
nessusagent-6.10.7-es7.x86_64.rpm	0ffec709084e91c5edc82480497841e3
nessusagent-6.10.7-fc20.x86_64.rpm	e4bdb71ccf6322d07a140128c9e6d448
nessusagent-6.10.7-suse11.i586.rpm	39fa63f40585ac9c6a4cc5bd49c10416
nessusagent-6.10.7-suse11.x86_64.rpm	a32642780c3cfdcd4786b95711b392d2
nessusagent-6.10.7-suse12.x86_64.rpm	a5e7e2fb155316db56bfe1fd84fe658d

File	MD5
nessusagent-6.10.7-ubuntu1110_amd64.deb	6784fb3ef79a98199285816972bf62e5
nessusagent-6.10.7-ubuntu1110_i386.deb	4074d5b209291b67d10dfd70acb994ab
nessusagent-6.10.7-ubuntu910_amd64.deb	0be545a957e274b8e129bfe5e5144960
nessusagent-6.10.7-ubuntu910_i386.deb	deea1711e57ced82fa41fc089e335b2b
nessusagent-6.10.7-Win32.msi	94683c259c9cae34de999007f8f1ec33
nessusagent-6.10.7-x64.msi	797c71afd810073ac4df374fabc96711

Nessus 6.10.8 Release Notes - 6/21/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix Nessus service crashes during scans

New Features/Expanded Platform Support

- Scan peered VPCs in a single pre-auth AWS scanner

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.8-amzn.x86_64.rpm	ec8628cc90a97ce9f061d4892db583e1
nessus-6.10.8-amzn.x86_64.rpm	f73ccee684a26efc1b3b149076b70637
nessusagent-6.10.8-debian6_amd64.deb	674f39b3f25dd2752d9955380021cb8f
nessus-6.10.8-debian6_amd64.deb	7f385391bf114ed2e09da353ef07da60
nessusagent-6.10.8-debian6_i386.deb	ab5068b9a26a7096b025c4344bb3c515
nessus-6.10.8-debian6_i386.deb	050ec6d1b55adf5d2801069772201a1d
nessusagent-6.10.8-es5.x86_64.rpm	e89e4ea0d6163c5c9dd44b5d81a88203
nessus-6.10.8-es5.x86_64.rpm	40479eb36c6044f45081cb3613a59bec

File	MD5
nessusagent-6.10.8-es5.i386.rpm	63a2ec12b66c5c72164a5892189a9dd2
nessus-6.10.8-es5.i386.rpm	8460356ae428b98d4af096e15daa23df
nessusagent-6.10.8-es6.x86_64.rpm	3d2d9ecb2b1906355646917e9c1063dd
nessus-6.10.8-es6.x86_64.rpm	c41ad34b094d132fc26f4618051ae801
nessusagent-6.10.8-es6.i386.rpm	7c122b1ee15aee95d745b68fe0214707
nessus-6.10.8-es6.i386.rpm	9f15d3871fb673dc396f482b2e8da3c4
nessusagent-6.10.8-es7.x86_64.rpm	7d3ee804e4813beaea8ee916c7c82e46
nessus-6.10.8-es7.x86_64.rpm	6f2c60c817a143f7b8f550866131a202
nessus-6.10.8-fbsd10-amd64.txz	7b92672c84fae13c55ca81f7d136d228
nessusagent-6.10.8-fc20.x86_64.rpm	e75ec3a03d071baee23d43080be252f5
nessus-6.10.8-fc20.x86_64.rpm	ea16b0857668e51e460def739ead459d
nessusagent-6.10.8.dmg	50b5d34202d47fa85abe6d907cb74807
nessus-6.10.8.dmg	1ecfbad7223a9f2d9b1bf68e7877ace0
nessusagent-6.10.8-suse11.x86_64.rpm	60d9f8a0390b44904da1a281180e688f
nessus-6.10.8-suse11.x86_64.rpm	3d132d3719cb825895759db387a6a6a4
nessusagent-6.10.8-suse11.i586.rpm	1d09a906d8e67ca24d23d1d57b1354ed
nessus-6.10.8-suse11.i586.rpm	31562476cafe1ad559caf85427aa1fa5
nessusagent-6.10.8-suse12.x86_64.rpm	0bd3c944db18ac579ceb72a266839b1d
nessus-6.10.8-suse12.x86_64.rpm	e85da19cda18fcbdf9dcf162ee0a9108
nessusagent-6.10.8-ubuntu1110_amd64.deb	ab3a6d19a4e97e672bdce51cb874f697
nessus-6.10.8-ubuntu1110_amd64.deb	303652308678baa3c6808960ff9ac1e7
nessusagent-6.10.8-ubuntu1110_i386.deb	f720b1c367b8adf775d7d2099bf53966

File	MD5
nessus-6.10.8-ubuntu1110_i386.deb	0e4cad2dc78e32773400d143bc0dfc1b
nessusagent-6.10.8-ubuntu910_amd64.deb	52744cf4c9659aa180d6ff96deabc4d4
nessus-6.10.8-ubuntu910_amd64.deb	b6fb60da6078cc4d1c455ff26aa6d82d
nessusagent-6.10.8-ubuntu910_i386.deb	df519006349768f4a44e6913e200bc59
nessus-6.10.8-ubuntu910_i386.deb	5447ab1cede9c7db8211de6ccff01898
nessusagent-6.10.8-Win32.msi	c44e0b82610c62e622e7bc877a235573
nessusagent-6.10.8-x64.msi	0d4f37852fd278358292a69d39627471
nessus-6.10.8-Win32.msi	1059da4ce078d7b6f7ead0f3297bf03d
nessus-6.10.8-x64.msi	6d2e0798fd1ddf4ee9d2faa3cd923ec4

Nessus 6.10.9 Release Notes - 7/14/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features/Expanded Platform Support

- Enable remote scanners to utilize bulk API for task updates

File Names & MD5 Checksums

File	MD5
nessus-6.10.9-amzn.x86_64.rpm	fd079491037c14c6f0bc049355346f1e
nessus-6.10.9-debian6_amd64.deb	80da540fd6744e47a5568c351045c5bb
nessus-6.10.9-debian6_i386.deb	f13ae198c4d69fa0410dd5aff979121c
nessus-6.10.9.dmg	84372a96209c2e729f7cd6325eb50425
nessus-6.10.9-es5.i386.rpm	dec894a59be7fac5cb915a7e1c46b060
nessus-6.10.9-es5.x86_64.rpm	a30dca1fc63a81d292e93bfae70f00e9

File	MD5
nessus-6.10.9-es6.i386.rpm	da3db47ac264b59dafdc8618a61b63ef
nessus-6.10.9-es6.x86_64.rpm	f99d05ed3f19e12c99fba2fa854af444
nessus-6.10.9-es7.x86_64.rpm	a748cd312ce7af14fa16f0eacab159df
nessus-6.10.9-fbsd10-amd64.txz	b084ffdd2157d3710b5c9b08e92ca0a2
nessus-6.10.9-fc20.x86_64.rpm	2e8a750b50fd803b8fa533dba98d1731
nessus-6.10.9-suse11.i586.rpm	4f170a88dfaba0e992705a625ebee3bc
nessus-6.10.9-suse11.x86_64.rpm	a1aa9ff5e70de93ed6bda4ff0601b796
nessus-6.10.9-suse12.x86_64.rpm	53fc22ae118d1d5646e145dd3eaca2c0
nessus-6.10.9-ubuntu1110_amd64.deb	5bb4a5bbb4d9c75b46b927da5846bc82
nessus-6.10.9-ubuntu1110_i386.deb	18a3932499f1d4f751ccca8b6f76ee8e
nessus-6.10.9-ubuntu910_amd64.deb	b232be5fd3f4ead180bc8273d8a66fde
nessus-6.10.9-ubuntu910_i386.deb	59a5ae6aeab2decf807dce102bee5054
nessus-6.10.9-Win32.msi	e4d106f97d967bb52e1a89d95c4b38a6
nessus-6.10.9-x64.msi	1d346f54b1a0322b25b9dc119f3d80d4
nessusagent-6.10.9-amzn.x86_64.rpm	4f4d86abedaa5017f72e339d43d1102d
nessusagent-6.10.9-debian6_amd64.deb	f0497bbb89979bb779b3dbd7ed4dd193
nessusagent-6.10.9-debian6_i386.deb	a888e7d4d32a917f360244fc6e031385
nessusagent-6.10.9.dmg	1ce564f6dfaa878963b0fc1551ad6bad
nessusagent-6.10.9-es5.i386.rpm	769cc48c1d01e96fadff9e4978372b36
nessusagent-6.10.9-es5.x86_64.rpm	7d9990e5c6454256c1b272acbec7e63f
nessusagent-6.10.9-es6.i386.rpm	967307cce60fbc7b3064ff360e56ac88
nessusagent-6.10.9-es6.x86_64.rpm	c2452077cfc57a95ba89437c809b82e4

File	MD5
nessusagent-6.10.9-es7.x86_64.rpm	a05da90ed88e6eaa4d67db144dfa2009
nessusagent-6.10.9-fc20.x86_64.rpm	70328eebe02c5fca33d5f69456abf471
nessusagent-6.10.9-suse11.i586.rpm	ff01840d6b7b03f3d4388bd128d3c7e4
nessusagent-6.10.9-suse11.x86_64.rpm	ad50e21cf77c6cf1f58e83a4620a770d
nessusagent-6.10.9-suse12.x86_64.rpm	7a8492bb7e2b5bf4414ff541cbe92b0f
nessusagent-6.10.9-ubuntu1110_amd64.deb	fbdff960ab6ab75a8ef1f3226109babc
nessusagent-6.10.9-ubuntu1110_i386.deb	81a5d3e38f18ee315e6cb9ee9b772d04
nessusagent-6.10.9-ubuntu910_amd64.deb	98fef19a5b61639289cba06492be3526
nessusagent-6.10.9-ubuntu910_i386.deb	d204bf38d9be5894fc08e5a9aafdf9f1
nessusagent-6.10.9-Win32.msi	964408138ddfacb6a9b1c507b62133ea
nessusagent-6.10.9-x64.msi	4b2fb90f9709b1a39e2e0dc2dabeb84d

Nessus 6.11.0 Release Notes - 8/7/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features/Expanded Platform Support

- Nessus Pro and Manager frontend mirror Tenable Vulnerability Management frontend
- Differential plugin updates
- Add support for SNI TLS extensions

Bug Fixes and Improvements

- Pagination for AWS pre-auth scanner for VPC peering support
- AWS scanners automatically apply security updates
- Proxy support for fetching updates for Amazon Linux
- Add support for SNI TLS extensions

- WannaCry template adjustment to disable brute force
- Resolved issue updating plugins through proxy

File Names & MD5 Checksums

File	MD5
nessus-6.11.0-amzn.x86_64.rpm	9e13b430642e16f9177109574a505c38
nessus-6.11.0-debian6_amd64.deb	a47e90c5182a55ff608e8135d99bfbb3
nessus-6.11.0-debian6_i386.deb	0171c31808e78b5edbe778df76b19000
nessus-6.11.0.dmg	e96c4803aab1d525e502e62b6794e9ce
nessus-6.11.0-es5.i386.rpm	5ab03802b25716c279010678a59e4700
nessus-6.11.0-es5.x86_64.rpm	09cc9d8d70fb14d907755cf5508ea5b6
nessus-6.11.0-es6.i386.rpm	4df5cf5327c57cc70bd4f33b73b18cfb
nessus-6.11.0-es6.x86_64.rpm	f6ace8ac8a3c721fb2d221b1b7034252
nessus-6.11.0-es7.x86_64.rpm	0a193650abec55a33b63bb214e2d62eb
nessus-6.11.0-fbsd10-amd64.txz	8f84007ccad852d1151a242c7297b450
nessus-6.11.0-fc20.x86_64.rpm	68f6fbd261d83ec60d64250091cd048f
nessus-6.11.0-suse11.i586.rpm	c398740c3b19d5e994aa56bb10c76e11
nessus-6.11.0-suse11.x86_64.rpm	b83cc16488b291c18261e1d0811283be
nessus-6.11.0-suse12.x86_64.rpm	cd59d4b611bf90687da96932008d69bf
nessus-6.11.0-ubuntu1110_amd64.deb	ecadca324fafa6d5eff42a096342c1ea
nessus-6.11.0-ubuntu1110_i386.deb	17303ca384fae801c129844bf7b0f467
nessus-6.11.0-ubuntu910_amd64.deb	81f16c3db34b921e07016df927f6f5d3
nessus-6.11.0-ubuntu910_i386.deb	f1d47f1f84ccb756be3c2bfa438dc22e
nessus-6.11.0-Win32.msi	7cada86acfc4abc6dfd239e4fea1d251
nessus-6.11.0-x64.msi	3e80d0c28c303ab3e6ef1a289657d2ad

File	MD5
nessusagent-6.11.0-amzn.x86_64.rpm	5ed4ebc5256f8fca11d59f5a49acad2c
nessusagent-6.11.0-debian6_amd64.deb	fcd57ff51f1c0bedfa489527e34b759f
nessusagent-6.11.0-debian6_i386.deb	d4313e4d685201e192173f024044a8af
nessusagent-6.11.0.dmg	4194206e0e2a634c67066914b9a3102b
nessusagent-6.11.0-es5.i386.rpm	7d9a7745264002039780b9513f087d92
nessusagent-6.11.0-es5.x86_64.rpm	2466397c8348b9f2c7defc5cf774b620
nessusagent-6.11.0-es6.i386.rpm	09f243650e8841559273d119dcec4028
nessusagent-6.11.0-es6.x86_64.rpm	0d522b6f23c37a0dbbd78cfd4c855d71
nessusagent-6.11.0-es7.x86_64.rpm	aa17609e955fb4b5195a64ce093b6fb3
nessusagent-6.11.0-fc20.x86_64.rpm	12f1165799c82e984ce6d8059286777b
nessusagent-6.11.0-suse11.i586.rpm	d083d141ecf3604b4bfaea39bcc0544e
nessusagent-6.11.0-suse11.x86_64.rpm	f225d7e404b8abf755ae3127a564ffd7
nessusagent-6.11.0-suse12.x86_64.rpm	4625562c72e6e69c8ada305d0c1a1d33
nessusagent-6.11.0-ubuntu1110_amd64.deb	b2f8d489bf364ad6158b6318cf178013
nessusagent-6.11.0-ubuntu1110_i386.deb	00b0901d7e0cada6762ce5007c4a1b0d
nessusagent-6.11.0-ubuntu910_amd64.deb	75c805d90548984a56232e3e97c0ac54
nessusagent-6.11.0-ubuntu910_i386.deb	3fc31ccf5ffd383e275dc248706f106
nessusagent-6.11.0-Win32.msi	f021a354c8bdbf36e1c5f6579af31e95
nessusagent-6.11.0-x64.msi	5bec76958ddfb8e26063efe470510456
nessus-updates-6.11.0.tar.gz	e26d24e5920f9367e9af7ea312e1069b

Nessus 6.11.1 Release Notes - 8/14/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix issue causing Nessus scanners from SecurityCenter to crash
- Improved severity readability for color-blind users
- Fix scrolling issue on policy page
- Fix format on plugin publication dates

File Names & MD5 Checksums

File	MD5
nessus-6.11.1-amzn.x86_64.rpm	8c655e2f8eea93f2035e09c7a457597c
nessus-6.11.1-debian6_amd64.deb	57dd86eea8ca6cda122351c444109f97
nessus-6.11.1-debian6_i386.deb	2576e4b4afed54a5f51cb0c56beaa8c6
nessus-6.11.1-es5.x86_64.rpm	fc94f08d37004dade1df26680b98d17e
nessus-6.11.1-es5.i386.rpm	a144fdf2ea7eb69194f1f08668416aeb
nessus-6.11.1-es6.x86_64.rpm	5c85e77f829dae422d20ef48165234c0
nessus-6.11.1-es6.i386.rpm	713b1d56730b4737e87a8ec86397b1eb
nessus-6.11.1-es7.x86_64.rpm	2eea9492cd89335abed8e8ccf95efafb
nessus-6.11.1-fbsd10-amd64.txz	70bbdcbf3ee46556aa14f47d3c199db9
nessus-6.11.1-fc20.x86_64.rpm	1a10805c5fab8106e85936c393c66209
nessus-6.11.1.dmg	5c68e99b4feb340056767d712604e91b
nessus-6.11.1-suse11.x86_64.rpm	e1b06399993e6910537fbd2687920b4b
nessus-6.11.1-suse11.i586.rpm	a49a22b87e932cf57efad4948953d21d
nessus-6.11.1-suse12.x86_64.rpm	1fe5bdafc0f64bd1bd630018314364ef
nessus-6.11.1-ubuntu1110_amd64.deb	a6321eaec6015fcccfa9b581c30ad563

File	MD5
nessus-6.11.1-ubuntu1110_i386.deb	1d4f462fbe75ad1be98b5a7d656db0dd
nessus-6.11.1-ubuntu910_amd64.deb	76a1198ad54cc522c208d4f2c13abc2c
nessus-6.11.1-ubuntu910_i386.deb	31ed0a15d5eb2609a971a77c85c01237
nessus-6.11.1-Win32.msi	3e8d94e821f06135393d06af7f4ecff5
nessus-6.11.1-x64.msi	35de4c222891ae8a1be97dc7a29aaed4
NessusAgent-6.11.1-es5.x86_64.rpm	6c80764fb922800f99a07b992f1c1394
NessusAgent-6.11.1-es5.i386.rpm	5bf57be05543c2afee490d1ec9dbcba1
NessusAgent-6.11.1-es6.x86_64.rpm	ce16cb2eb66ab5546a8d8bb89231fd2a
NessusAgent-6.11.1-es6.i386.rpm	8b1e2ff08b845353c0242b676cf2de38
NessusAgent-6.11.1-es7.x86_64.rpm	bfbbfbcf6f9204711ab01cd17d328e17
NessusAgent-6.11.1-fc20.x86_64.rpm	bdd4efea8c8cf7a621be15b4a2e92b2d
NessusAgent-6.11.1.dmg	ddec71833f127d4a5be8350fa01f7a76
NessusAgent-6.11.1-suse11.x86_64.rpm	629ef898bf8cf49706a48938e503e3f4
NessusAgent-6.11.1-suse11.i586.rpm	f6466c9acb8d0bd7ce9f4a72705f256f
NessusAgent-6.11.1-suse12.x86_64.rpm	7de30047bdbffa88266d4e097e9191cb
NessusAgent-6.11.1-ubuntu1110_amd64.deb	f71d34599cac4ce657bc4c47a5b583c2
NessusAgent-6.11.1-ubuntu1110_i386.deb	0b51f3fcf31ba7e04962608060c61cea
NessusAgent-6.11.1-ubuntu910_amd64.deb	b35795c3086fecb18d8bb61c898e3e0b
NessusAgent-6.11.1-ubuntu910_i386.deb	61f931b7b96d97754548464000388 3f5
NessusAgent-6.11.1-Win32.msi	c073a38637a46ce1ccbab2576ee1f47c
NessusAgent-6.11.1-x64.msi	7fdfe41cec26cc5db994b4bb11e3566a
nessus-updates-6.11.1.tar.gz	371aef3d2c61c169ce2c37397c7a1e65

Nessus 6.11.2 Release Notes - 10/26/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Update bulkUpdate to improving scalability
- Allow scan results summary to be printable from on-screen
- Fix checkbox to copy scan history

File Names & MD5 Checksums

File	MD5
nessus-updates.tar.gz	a2e7f0dcf3cf8d2244aa88f3dfedbe01
NessusAgent-6.11.2-amzn.x86_64.rpm	d7601087c2ad8286cdffdbff55d9032e
Nessus-6.11.2-amzn.x86_64.rpm	b61587b0a7cca39d24d0891c9c4c4576
NessusAgent-6.11.2-debian6_amd64.deb	d769e713c307c5264eff25541e097737
Nessus-6.11.2-debian6_amd64.deb	70220c6a1dde89eec00c231787316d46
NessusAgent-6.11.2-debian6_i386.deb	58bce5c1f8b177659806a25c46fac672
Nessus-6.11.2-debian6_i386.deb	1af8f76684d5769c91aa0fc7972ae02c
NessusAgent-6.11.2-es5.x86_64.rpm	b7ad5bb3911229c3ff6ca09738283855
Nessus-6.11.2-es5.x86_64.rpm	74a096aff3b5f9be1630f95bd8710855
NessusAgent-6.11.2-es5.i386.rpm	5f0ade7cdbc877e76a6195064e41a890
Nessus-6.11.2-es5.i386.rpm	ae08e1c0ababd5040287b4d606428e05
NessusAgent-6.11.2-es6.x86_64.rpm	8f987543484206bd653549a497e5a414
Nessus-6.11.2-es6.x86_64.rpm	6f9e8b7f713fe77cc9f46143dd797f41
NessusAgent-6.11.2-es6.i386.rpm	660478368c5553544ff6c990338fd8a2
Nessus-6.11.2-es6.i386.rpm	ebfbc288ee55217888d1fdde456baa61
NessusAgent-6.11.2-es7.x86_64.rpm	956c220467011548b2a0800c4aa2299e

File	MD5
Nessus-6.11.2-es7.x86_64.rpm	402ca3836abc17d01f83a67af62f9806
Nessus-6.11.2-fbsd10-amd64.txz	6c49ce1b04563ce41a572f61c79b59b9
NessusAgent-6.11.2-fc20.x86_64.rpm	0bbb1d2c96cd85161333ab57cb309222
Nessus-6.11.2-fc20.x86_64.rpm	4c4cb919710b76003e685c41821ef928
NessusAgent-6.11.2.dmg	7ca45e2861f71fb54a8b9ccf2a4f6db0
Nessus-6.11.2.dmg	8d3c488b4e9be2c3638ca7eb602f48c4
NessusAgent-6.11.2-suse11.x86_64.rpm	0e8e4d019a557e1050a93bfdcc0d6e60
Nessus-6.11.2-suse11.x86_64.rpm	0957a7faba4410bf3b0885fd48b1aa22
NessusAgent-6.11.2-suse11.i586.rpm	a67ee214ac52bc118b84b8bc2a81d10b
Nessus-6.11.2-suse11.i586.rpm	3ab6f4ed5eb2ce2619c33f11ff58ab52
NessusAgent-6.11.2-suse12.x86_64.rpm	ceb4b692f44b8710de981e8ada360fc2
Nessus-6.11.2-suse12.x86_64.rpm	14c5913f2e5d78ccc1a7f4dc7b337ad0
NessusAgent-6.11.2-ubuntu1110_amd64.deb	dc1fb093506c992a961c1c19bbdb61b0
Nessus-6.11.2-ubuntu1110_amd64.deb	3c792c1d698a65e841470831c2ca032e
NessusAgent-6.11.2-ubuntu1110_i386.deb	d93e2198f70c42a813ed7c8cad3ac9cb
Nessus-6.11.2-ubuntu1110_i386.deb	c9ba83faa87b8b9098f50e9a89ca8f2f
NessusAgent-6.11.2-ubuntu910_amd64.deb	f4c367bc1414a6cfdbb478a2e4ea7390
Nessus-6.11.2-ubuntu910_amd64.deb	19555d3d06bb9c0511d4f5b8612576d4
NessusAgent-6.11.2-ubuntu910_i386.deb	207e73ec3644eabf175d65fd03ae0eba
Nessus-6.11.2-ubuntu910_i386.deb	9d10b733c653f90c7d5ca05941fdf866
NessusAgent-6.11.2-Win32.msi	75a4492653bc744be12fcc8f47154481
NessusAgent-6.11.2-x64.msi	2ddae89d1985c814791e7c47a7c4294f

File	MD5
Nessus-6.11.2-Win32.msi	ca17a06bd2e7f761940a50c306250940
Nessus-6.11.2-x64.msi	5f61b7b7cc18f159d1f673786ecb8673

Nessus 6.11.3 Release Notes - 12/5/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix for IAVM 2017-A-0327 Multiple Vulns in OpenSSL
- Fix to display latest version update in-product banner

File Names & MD5 Checksums

File	MD5
Nessus-6.11.3-amzn.x86_64.rpm	65a8df09eba93e239df1aa5e1948d1d6
Nessus-6.11.3-debian6_amd64.deb	f62355b2c53a1752ce752b187b6c4a33
Nessus-6.11.3-debian6_i386.deb	0cc4f2087c7a03ab40be9a9447333a00
Nessus-6.11.3-es5.x86_64.rpm	133208d3afe0b33dbc57d2bf89891d58
Nessus-6.11.3-es5.i386.rpm	d6e034eff3b9c379aedcbec6d99931bb
Nessus-6.11.3-es6.x86_64.rpm	e0a9fe66bf6f22e5988758c87ef94e46
Nessus-6.11.3-es6.i386.rpm	b622df955f39919c91501ff65aaa389e
Nessus-6.11.3-es7.x86_64.rpm	f5aaa9dfb53ab3f1eb8b323956f7e6c2
Nessus-6.11.3-fbsd10-amd64.txz	b76bee04786e63ad8b062051c8c9ce29
Nessus-6.11.3-fc20.x86_64.rpm	669536281a2a9df87cf9b793338fac08
Nessus-6.11.3.dmg	49129fb7da9315bc6fad4a9513a65f08
Nessus-6.11.3-suse11.x86_64.rpm	86aebda4839c156c3ddcb768ca76e09b

File	MD5
Nessus-6.11.3-suse11.i586.rpm	ef0707b52ed7b1dd63bf0795e22112fd
Nessus-6.11.3-suse12.x86_64.rpm	ee5d3c1be707fc583624e2f4a18cf104
Nessus-6.11.3-ubuntu1110_amd64.deb	42e6ca8376e188eb4a8e7d24c0487091
Nessus-6.11.3-ubuntu1110_i386.deb	b243df5259e7eba79a2b8b33da93238a
Nessus-6.11.3-ubuntu910_amd64.deb	9542da761b3744d40819e889e10374db
Nessus-6.11.3-ubuntu910_i386.deb	dd268ad6b47c7a54850cf72481a0b631
Nessus-6.11.3-Win32.msi	b3886684faea52a6c8d70a5eb994d60b
Nessus-6.11.3-x64.msi	4e9a2e249a59dce1d473fabcead1b7b9

Nessus 7.0.0 Release Notes - 12/12/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

New Features, Improvements and Expanded Platform Support

- Enable easy license transfer across multiple devices
- Allow for custom name and logo on reports
- Specify email recipient for completed scan reports
- Opt in/out of Nessus Pro v7 features
- Onboarding improvements
- Updated design of HTML and PDF reports
- Instrumentation to measure users on new version

- Update all icons and name for Nessus Pro v7
- Nessus Home and Eval update to reflect new experience

Changed Functionality

- Remove the ability to add additional users - Nessus Pro Only
- Restrict scan API capabilities - Nessus Pro Only

Bug Fixes

- Sideloading plugins from SC causes Nessus license downgrade
- AWS VPC peering connection fix
- Modifying plugin severity affects all hosts in a scan
- Offline registration feed error
- Severity filter fix
- Scans page filter reset fix
- Fix “Show Enabed” link
- Firefox display fixes
- Unable to delete scans if sharing is enabled
- Nessus 6.11 page rendering issues

File Names & MD5 Checksums

File	MD5
NessusAgent-7.0.0-amzn.x86_64.rpm	c8cc067b21925fe7f435b79276199ed4
Nessus-7.0.0-amzn.x86_64.rpm	3f8d57da40ffd5dc757a3264e4701a38
NessusAgent-7.0.0-debian6_amd64.deb	48d426900392dee9e107e56ed78f9c40
Nessus-7.0.0-debian6_amd64.deb	d1dd1d4b10d6b503d1593e87bfd5ca05
NessusAgent-7.0.0-debian6_i386.deb	37445ece0f6cbc57ed4150630ef8d836
Nessus-7.0.0-debian6_i386.deb	5844092de3277355266e6de31a43e263

File	MD5
NessusAgent-7.0.0-es5.x86_64.rpm	af9ec38ed8e9a0ae37af7aa21a38e09c
Nessus-7.0.0-es5.x86_64.rpm	83c8accec624148ff8aef9b7ab56ef8b
NessusAgent-7.0.0-es5.i386.rpm	6d143848f4f4748722261e27232328fb
Nessus-7.0.0-es5.i386.rpm	59f0194e18b6c32f8a59fcf56195d3d4
NessusAgent-7.0.0-es6.x86_64.rpm	47b14b32086a8acb4b25c09ad3f801b1
Nessus-7.0.0-es6.x86_64.rpm	fb26a57df7d5dacebdcc0063e6a8cac4
NessusAgent-7.0.0-es6.i386.rpm	cd5f1f52a80cc383f96d858c205a0769
Nessus-7.0.0-es6.i386.rpm	47e92bda68167bd732ce6e6e5922bbfa
NessusAgent-7.0.0-es7.x86_64.rpm	4f1e9bb8963e2530f338014df5bda9de
Nessus-7.0.0-es7.x86_64.rpm	f168fdfdfe5b7298bb562d51272afe33
Nessus-7.0.0-fbsd10-amd64.txz	0895a234df2a031bc8b5dff5e03a0f33
NessusAgent-7.0.0-fc20.x86_64.rpm	b9a8456147fa4ecf1935b536453b4a42
Nessus-7.0.0-fc20.x86_64.rpm	970a213e9bcee4ad3b93f666f89d1128
NessusAgent-7.0.0.dmg	825afa3c82ec4790f75029e8f2a94c01
Nessus-7.0.0.dmg	0126b4635b91dacdc66109ebaecde7bd
NessusAgent-7.0.0-suse11.x86_64.rpm	7ea534e85cadeeeabb755136674638e9
Nessus-7.0.0-suse11.x86_64.rpm	b3503efabd80d06d1e16dc8df56e1bbb
NessusAgent-7.0.0-suse11.i586.rpm	53aec1d4d0b9917933a18e453348b9b1
Nessus-7.0.0-suse11.i586.rpm	e553ebe285c37b1723d8e5a6f8d152d2
NessusAgent-7.0.0-suse12.x86_64.rpm	6f68476136bd7b42c2c4ca33b0fdfd04
Nessus-7.0.0-suse12.x86_64.rpm	005fd028422fdda24bd89ac6fea504cd
NessusAgent-7.0.0-ubuntu1110_amd64.deb	050b98d68843d984872de7a9c6d3a87c

File	MD5
Nessus-7.0.0-ubuntu1110_amd64.deb	ccafd1edc0356023b0cd9f0ca7486164
NessusAgent-7.0.0-ubuntu1110_i386.deb	d8b456473f0e8821797277c4446125df
Nessus-7.0.0-ubuntu1110_i386.deb	cd185f20082e45858080edd37dbdf394
NessusAgent-7.0.0-ubuntu910_amd64.deb	1d5cf07078e1943f3a6ebbed7863415e
Nessus-7.0.0-ubuntu910_amd64.deb	3b0dab44ffe591a367cd3bab09841a18
NessusAgent-7.0.0-ubuntu910_i386.deb	bc5ee800c7ed54efd8f4ab4a7167f24b
Nessus-7.0.0-ubuntu910_i386.deb	3cd2ee15025c097b7d03bbf41490b05a
NessusAgent-7.0.0-Win32.msi	e57633b478f3ebbbd91d5bf158aef684
NessusAgent-7.0.0-x64.msi	a4b6895f799853b99c0e4c662cf35eca
Nessus-7.0.0-Win32.msi	35f63ac61b0a250332e6b2817c40ad81
Nessus-7.0.0-x64.msi	884c30fb22ca4db03370ecc509053e7e

2016 Tenable Nessus

Nessus 6.5.5 Release Notes - 2/15/2016

Nessus 6.5.6 Release Notes - 3/2/2016

Nessus 6.6.0 Release Notes - 4/11/2016

Nessus 6.6.1 Release Notes - 4/20/2016

Nessus 6.6.2 Release Notes - 4/27/2016

Nessus 6.7.0 Release Notes - 5/19/2016

Nessus 6.8.0 Release Notes - 7/19/2016

Nessus 6.8.1 Release Notes - 7/25/2016

Nessus 6.9.0 Release Notes - 10/25/2016

Nessus 6.9.1 Release Notes - 11/9/2016

Nessus 6.9.2 Release Notes - 12/14/2016

Nessus 6.5.5 Release Notes - 2/15/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix cross-site scripting errors in the Nessus UI (see Tenable Product Security Advisory TNS-2016-02)

File Names & MD5 Checksums

File	MD5
Nessus-6.5.5-debian6_amd64.deb	e2594b02f1e146814fa9bde7be2a453a
Nessus-6.5.5-debian6_i386.deb	26ee5f37cee3986910f14d2ead578445
Nessus-6.5.5.dmg	bb3714841a97ae78ed485819acfe5b0d
Nessus-6.5.5-es5.i386.rpm	4619e0402edb0f51a3fd6249a179a76a
Nessus-6.5.5-es5.x86_64.rpm	75797d38b3997e0d3eccc59cb90d6043
Nessus-6.5.5-es6.i386.rpm	a731a1d6e8b3be13eb233d43174a75f6
Nessus-6.5.5-es6.x86_64.rpm	5d2506af40c0be58186492b3635eb7a4
Nessus-6.5.5-es7.x86_64.rpm	91229f18af5570290a7d3ad8b0e5de46
Nessus-6.5.5-fbsd10-amd64.txz	fde1f4dc4a68dcd29cd6c883a0a02a49
Nessus-6.5.5-fc20.x86_64.rpm	a7bfb352df694a752e4fdfedc688f116
Nessus-6.5.5-suse10.x86_64.rpm	14c97620ab679b3dab9fdd5c20628749
Nessus-6.5.5-suse11.i586.rpm	66818d7905c511b13430e6d8cd11af97
Nessus-6.5.5-suse11.x86_64.rpm	54f09a889abfa3b67a238cfb41b4d36d
Nessus-6.5.5-ubuntu1110_amd64.deb	af4c0b745b439ae3b8a0ba2cf77804f1
Nessus-6.5.5-ubuntu1110_i386.deb	0b7dd45113ddd8b0968df5a9d1eb290b
Nessus-6.5.5-ubuntu910_amd64.deb	53236f4dbc6638710c4d9aef3accdf41

File	MD5
Nessus-6.5.5-ubuntu910_i386.deb	c446f2aa5d0600cdaf01af96ce52178d
Nessus-6.5.5-Win32.msi	6ba8af99ab1e5da00f77296ca649ee93
Nessus-6.5.5-x64.msi	b347d4eb0614d01f999ff8b1d5b81374
NessusAgent-6.5.5-amzn.x86_64.rpm	44d98abe8709804358e5194d534f146c
NessusAgent-6.5.5-debian6_amd64.deb	1ec06a2b6d83c20f72b775d3a27f529e
NessusAgent-6.5.5-debian6_i386.deb	f16b57a86d301ecf188b551159aa2758
NessusAgent-6.5.5.dmg	dde2b5006a1cbb168b9a3b2216b41ef0
NessusAgent-6.5.5-es5.i386.rpm	07c899a9dad20f8cdf7707625be03eb9
NessusAgent-6.5.5-es5.x86_64.rpm	3523dc6a3b84020666cf13941ab9200e
NessusAgent-6.5.5-es6.i386.rpm	709fd684662ba67bb7e7a119706b1784
NessusAgent-6.5.5-es6.x86_64.rpm	e1aedbdc6c73e5dce4dfe30cb731a009
NessusAgent-6.5.5-es7.x86_64.rpm	f7dab26a9ee4b222ac677b7fdfcd4c78
NessusAgent-6.5.5-fc20.x86_64.rpm	d4bbe71d06f51c18dca4cc672d2b2635
NessusAgent-6.5.5-ubuntu1110_amd64.deb	d0b78227b1af298f18028a4a81b1aeee
NessusAgent-6.5.5-ubuntu1110_i386.deb	cda7ebeb2cfffff13ce0fbe3460426b3
NessusAgent-6.5.5-ubuntu910_amd64.deb	4e32618f75c1b37399c4cc3c5e3e72ba
NessusAgent-6.5.5-ubuntu910_i386.deb	2c0c5e5cb957a34690dd2ccb580ca758
NessusAgent-6.5.5-Win32.msi	8763cd17b6476deb6be83e5da5934205
NessusAgent-6.5.5-x64.msi	e46d1017b67d12f1c396c035d6806321

Nessus 6.5.6 Release Notes - 3/2/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features/Expanded Platform Support

- New scanning template for the DROWN vulnerability

Bug Fixes and Improvements

- Update OpenSSL to 1.0.1s (see Tenable Product Security Advisory TNS-2016-03)

File Names & MD5 Checksums

File	MD5
Nessus-6.5.6-debian6_amd64.deb	8fb662b3855395685b44f4cb30d7eded
Nessus-6.5.6-debian6_i386.deb	6fcf88fd3c12715920a4182f5ed020a3
Nessus-6.5.6.dmg	005188f4525d0229690bad1c8f74bb20
Nessus-6.5.6-es5.i386.rpm	9b71fb1c8cf483fcb1ce753000b30fda
Nessus-6.5.6-es5.x86_64.rpm	9637dbbc2414519fe76c8349d846da41
Nessus-6.5.6-es6.i386.rpm	50ada4f27e2539664b7a5f31c519103e
Nessus-6.5.6-es6.x86_64.rpm	1b25a28361bc735b9ea9b5f6771c6440
Nessus-6.5.6-es7.x86_64.rpm	8063b5f79cb62a79250f228c267f78b8
Nessus-6.5.6-fbsd10-amd64.txz	d189ceb3d1d5628d2d00a44d99bde855
Nessus-6.5.6-fc20.x86_64.rpm	7dc3a305dfb5d9e8f020483b4b6d45d0
Nessus-6.5.6-suse10.x86_64.rpm	9887f05a63abe131b8ded26027d3932f
Nessus-6.5.6-suse11.i586.rpm	f18502ddcc5537f13cab46f1b1ff4628
Nessus-6.5.6-suse11.x86_64.rpm	fb81ef290557844f51ec4f0c0463937b
Nessus-6.5.6-ubuntu1110_amd64.deb	8dcc76c7e75019d08ea67ea9a9172fe6
Nessus-6.5.6-ubuntu1110_i386.deb	2e926297d31fc44689cb484ef379bfdc
Nessus-6.5.6-ubuntu910_amd64.deb	0c581695a03d9190c14cecb650afd6c4
Nessus-6.5.6-ubuntu910_i386.deb	30a59e2f86d275abfeccceaf353f5df1
Nessus-6.5.6-Win32.msi	4671ec9a4505e93bd78376fd34431548
Nessus-6.5.6-x64.msi	cbb24560465ace8207f0e89c146b7a2c

File	MD5
NessusAgent-6.5.6-amzn.x86_64.rpm	8b6adcb16c4d4d35711fca80fa6c3a61
NessusAgent-6.5.6-debian6_amd64.deb	a1f656b26f951a4a89a52dcd2ba904de
NessusAgent-6.5.6-debian6_i386.deb	649a05874d6d3fc37a02e5e2d06f9715
NessusAgent-6.5.6.dmg	8e4f9fd79816a9550bf2bcf6517eca5e
NessusAgent-6.5.6-es5.i386.rpm	4bf907269bf6e82d94dc8bc43be14fce
NessusAgent-6.5.6-es5.x86_64.rpm	b84a7311a5dd8ee4cd07b574bcef1a69
NessusAgent-6.5.6-es6.i386.rpm	a3515e274ac2da260924586fc00ee575
NessusAgent-6.5.6-es6.x86_64.rpm	e1299a6c1597178ca367eaf7b181ce1a
NessusAgent-6.5.6-es7.x86_64.rpm	f754769945bdc2a4df34de4e5db18725
NessusAgent-6.5.6-fc20.x86_64.rpm	7f3c30e861a5a8b9abf2cdbf7833e8e8
NessusAgent-6.5.6-ubuntu1110_amd64.deb	7a3ef3586a2fa29a6df6e1e61b3cc382
NessusAgent-6.5.6-ubuntu1110_i386.deb	3c36500f4fbc7976e7c2bf80dcb4a4ee
NessusAgent-6.5.6-ubuntu910_amd64.deb	31a5d2af845142bb67350129e8b8a243
NessusAgent-6.5.6-ubuntu910_i386.deb	511f1ea0590e96429de0182d42bafef1
NessusAgent-6.5.6-Win32.msi	cda4f4e7fdba194bce27cf8bd94dd952
NessusAgent-6.5.6-x64.msi	0e41e2d4365219a76335a1896a1b3873

Nessus 6.6.0 Release Notes - 4/11/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features / Improvements / Changes in Support

- Nessus Cloud UI Enhancements - improved workflow and dashboards
- Nessus Cloud no longer supports Internet Explorer 10 and under
- Nessus Agents now support running on Windows 10 and Debian 8

- Nessus Professional, Nessus Manager, and managed Nessus scanners now support running on Windows 10, Debian 8, and Kali 2.0
- Added the ability to detect malware on the filesystem
- Add the "Internal Network PCI Scan" template to Nessus Cloud
- Upgrade Nessus certificates to SHA-256

Bug Fixes

- Custom compliance audit info not showing in API call showing policy details
- Various related to Agent/Manager comms with IPv6 available
- Scan name missing from email subject and report on emailed Nessus Agent scan results
- Upgrade from 5.2.12 to 6.5 breaks a Host Discovery scan
- Don't unlink Windows Agent during upgrade if linked
- Fixes for IPv6-related issues on scanners
- Agents can link to manager via /etc/hosts entry, but will not receive scan jobs
- Nessus SYN scanner doesn't respect port rules
- Debian/Ubuntu init script status returning incorrect error code when Nessus is stopped
- Remote scanners don't update based on update commands issued on status page in Nessus Manager
- Submitting API request for PUT /policies with invalid format will incorrectly return HTTP OK (Status code 200)
- Offline Config Audit filenames not saving correctly after being changed
- Update Host Discovery templates to only use accounts specified in policy by default
- Plugin 46215 Inaccurate Output from Agent Scans
- XSS via import of malicious Nessus DB file
- Nessus server crash via XML entities processing bomb
- Aliasing additional IP Addresses results in Nessus agents reporting incorrect IP
- TCP Port Scans not working in Nessus Cloud

File Names & MD5 Checksums

File	MD5
Nessus-6.6.0-debian6_amd64.deb	9f0ba3f7e7dd080a8ddbc9ed2cc8e6c8
Nessus-6.6.0-debian6_i386.deb	1b5c53f94bc04a4a956de7726cbea0f8
Nessus-6.6.0.dmg	5f6e7b1807255abbc260fea8d2937ff6
Nessus-6.6.0-es5.i386.rpm	aa37d574b39e7d5462bc5063ef1259a0
Nessus-6.6.0-es5.x86_64.rpm	66d1f9cd931567a3f2f50485056495bc
Nessus-6.6.0-es6.i386.rpm	85dca2ef77542ece000d36f65d81ee5b
Nessus-6.6.0-es6.x86_64.rpm	47df8964dad686387d0e3b98ffa96670
Nessus-6.6.0-es7.x86_64.rpm	c8fde172a567eed75bbcc94415e9cb86
Nessus-6.6.0-fbsd10-amd64.txz	e7eb22b40bbb51c6e47039d175603796
Nessus-6.6.0-fc20.x86_64.rpm	d2da54786692f32e237da84f3fbab960
Nessus-6.6.0-suse10.x86_64.rpm	e2476b3bc49cfce2f5bb9651781570b7
Nessus-6.6.0-suse11.i586.rpm	5617d0d92dde670fa52f61653d5adb5f
Nessus-6.6.0-suse11.x86_64.rpm	0e7908b926d6ce9305f49c0ea03e0259
Nessus-6.6.0-ubuntu1110_amd64.deb	483f56b4753069056ae3d5d22659fc53
Nessus-6.6.0-ubuntu1110_i386.deb	1cdd2d4ef5cde5ef94197398acdb3b25
Nessus-6.6.0-ubuntu910_amd64.deb	c775aef9289bd2c3546fc02ea084d443
Nessus-6.6.0-ubuntu910_i386.deb	ab0d81170589d17703cfe55bcb80e723
Nessus-6.6.0-Win32.msi	bc8041d3787c5538fad449beaa26e3d0
Nessus-6.6.0-x64.msi	36d2d648e346f9b77733ed0c47549f8a
NessusAgent-6.6.0-amzn.x86_64.rpm	5bc34bb5e6dfb6bfcff562232cffc6eb
NessusAgent-6.6.0-debian6_amd64.deb	8909a24d4f95be54743e35a4ca29e561
NessusAgent-6.6.0-debian6_i386.deb	2ea5820ad2af7f44dbcd87841dc30ab8

File	MD5
NessusAgent-6.6.0.dmg	5fb033fcd8fb87070e88d0eebced8682
NessusAgent-6.6.0-es5.i386.rpm	5fb20d14c46ba251c5fffc418885bbc9
NessusAgent-6.6.0-es5.x86_64.rpm	d35e94e14277b453e728ab16fe7ec384
NessusAgent-6.6.0-es6.i386.rpm	f3631015601bcc87e11851ab31f12e30
NessusAgent-6.6.0-es6.x86_64.rpm	bec0fc1c79b570e79a1f131c0aca9e48
NessusAgent-6.6.0-es7.x86_64.rpm	07646d2a37058cffba10ba89b84126d6
NessusAgent-6.6.0-fc20.x86_64.rpm	ea4d64a7612d16bc3ba4cf97ad4757a1
NessusAgent-6.6.0-ubuntu1110_amd64.deb	c747d2149a94ed44b3ab180c4d6d7c3c
NessusAgent-6.6.0-ubuntu1110_i386.deb	27bdcb4cfe708dd390be24bae3caddd0
NessusAgent-6.6.0-ubuntu910_amd64.deb	9261d9658d60bff13be58a49b12cb28e
NessusAgent-6.6.0-ubuntu910_i386.deb	86a16bd6546ccf70761456247c7699a6
NessusAgent-6.6.0-Win32.msi	006551af5cbca9fc8da9395734b0a9f7
NessusAgent-6.6.0-x64.msi	65c3490b3d632b14fd7c84108883da47

Nessus 6.6.1 Release Notes - 4/20/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features / Expanded Platform Support

- Add policy and scan template for Badlock

Bug Fixes and Improvements

- Clarify UI wording regarding Nessus licenses for offline activation
- Fixed condition where spurious "decrementReference" errors were being logged to nessusd.dump

File Names & MD5 Checksums

File	MD5
Nessus-6.6.1-debian6_amd64.deb	2ba85ee3d01d55a3420c9085e0df5c8b
Nessus-6.6.1-debian6_i386.deb	05c1c4ae37be2c27c4fd6fbb28281ddb
Nessus-6.6.1.dmg	7e0676eee54ca83e929190105282869 3
Nessus-6.6.1-es5.i386.rpm	809887cc51e8b6d5445d0560ca61a955
Nessus-6.6.1-es5.x86_64.rpm	368aff9a415cf441f6a4a8043e4f5fab
Nessus-6.6.1-es6.i386.rpm	96c8f277e82015a79a00e2f99409b662
Nessus-6.6.1-es6.x86_64.rpm	02d530eeb6a748f33d9e3887c02051bd
Nessus-6.6.1-es7.x86_64.rpm	6b861c63346056a591149718a288988d
Nessus-6.6.1-fbsd10-amd64.txz	7a15cb8accfe804d856da6924f42485d
Nessus-6.6.1-fc20.x86_64.rpm	28f86ffcccf03cf87eab80e853fd8abf
Nessus-6.6.1-suse10.x86_64.rpm	e51cbb6201da5f46eeb20e6c9715ac50
Nessus-6.6.1-suse11.i586.rpm	fa4231b784da76e9c6a66ec3e2f0a922
Nessus-6.6.1-suse11.x86_64.rpm	add1abfc0ee98db1c98376741c427b9a
Nessus-6.6.1-ubuntu1110_amd64.deb	de985a028b816de5bd5afc96d6939fe9
Nessus-6.6.1-ubuntu1110_i386.deb	3b428856660941596c836a9443af1cfd
Nessus-6.6.1-ubuntu910_amd64.deb	0b6956904807d50ffc1053bb0caaee16
Nessus-6.6.1-ubuntu910_i386.deb	bc2d4ad99c46d767f42eb630e4d17ee9
Nessus-6.6.1-Win32.msi	f82ddd940eefd12e90538992162db63a
Nessus-6.6.1-x64.msi	207cd13bab2e12150c1c291b69d11742
NessusAgent-6.6.1-amzn.x86_64.rpm	366e9c67c54277881960c50569e4ad51
NessusAgent-6.6.1-debian6_amd64.deb	bd2eff18ea1743c9ecdbcce73a84c9d9
NessusAgent-6.6.1-debian6_i386.deb	0b285231bcf16c6d3b4187daa35adc5e

File	MD5
NessusAgent-6.6.1.dmg	6900819777acd81334963037b20743b1
NessusAgent-6.6.1-es5.i386.rpm	647e4d6b7c22e534c294ce1c92cf311f
NessusAgent-6.6.1-es5.x86_64.rpm	ddea81f7cb88e95e20306b610ffddf8a
NessusAgent-6.6.1-es6.i386.rpm	1390e09d887387b26578ca3d6dac6e62
NessusAgent-6.6.1-es6.x86_64.rpm	bd32d443ce69119fe3219876c61443fb
NessusAgent-6.6.1-es7.x86_64.rpm	42ffbd96d5adfa1004c46509e4496055
NessusAgent-6.6.1-fc20.x86_64.rpm	71617dffb2191c505733a6959e8392c3
NessusAgent-6.6.1-ubuntu1110_amd64.deb	77927d1c5699d179c9bd7436fd2e6d9b
NessusAgent-6.6.1-ubuntu1110_i386.deb	8ac2b53782daf7d3b1cf072c914ad651
NessusAgent-6.6.1-ubuntu910_amd64.deb	eb33846daa5840486717cd7928119a27
NessusAgent-6.6.1-ubuntu910_i386.deb	55681980928a173a00a321717359a0ef
NessusAgent-6.6.1-Win32.msi	34bafffe691eb5df8bbb62da32bef905
NessusAgent-6.6.1-x64.msi	2e49ecc45ce4246917b62636a232bd9b

Nessus 6.6.2 Release Notes - 4/27/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- On OS X, Nessus can consume 100% CPU when compiling plugins and not finish
- Ignore empty notification filters when building queries
- Settings for shared scans cannot be updated by a user with 'Can Configure' permissions
- Per-host licensing restrictions incorrectly being applied to Host Discovery scans

File Names & MD5 Checksums

File	MD5
Nessus-6.6.2-debian6_amd64.deb	d2229457e3d3a07dcf0a21110d1b6269
Nessus-6.6.2-debian6_i386.deb	582a578120c8937347d93af8353bc6f4
Nessus-6.6.2.dmg	420957bfb495984d9a1cf14e3b9145d9
Nessus-6.6.2-es5.i386.rpm	0ee451ba41a0e2baef6aff8afdbcc037
Nessus-6.6.2-es5.x86_64.rpm	59a482ccc6fbb5948cd78cd26ea80d47
Nessus-6.6.2-es6.i386.rpm	0aee43fddc39bc72a8f8723d9dee65d8
Nessus-6.6.2-es6.x86_64.rpm	9faec53025c5e8057d250508fc60640c
Nessus-6.6.2-es7.x86_64.rpm	bb37237ca70cd53478f6c9eb5cccf788
Nessus-6.6.2-fbsd10-amd64.txz	751501137a921119c2b9cb9d664a50b0
Nessus-6.6.2-fc20.x86_64.rpm	c65bc9706a7390f274428d688d705e95
Nessus-6.6.2-suse10.x86_64.rpm	b7fb05512493d28cde20fc43e467ad1c
Nessus-6.6.2-suse11.i586.rpm	06dd93260f1cf58e43a5d106eb4567f1
Nessus-6.6.2-suse11.x86_64.rpm	0d62ec1ec3460efeb419e49c317f2aea
Nessus-6.6.2-ubuntu1110_amd64.deb	5b04f74b4f63a2cf9c7192d27b5df209
Nessus-6.6.2-ubuntu1110_i386.deb	f5b32c766b78e78c68c3c8bba933966b
Nessus-6.6.2-ubuntu910_amd64.deb	78e18499aad700ec48cfc6fec0965bf0
Nessus-6.6.2-ubuntu910_i386.deb	add29e2e97d4879dfeb3461d95b01389
Nessus-6.6.2-Win32.msi	1159ea4259ace11d6756de7ff6f4061c
Nessus-6.6.2-x64.msi	6e711559d352828eb5198b85183cb726
NessusAgent-6.6.2-amzn.x86_64.rpm	461c55794fb09c38769a482ce7184298
NessusAgent-6.6.2-debian6_amd64.deb	b450324913a3335de9544e3221a15cf7
NessusAgent-6.6.2-debian6_i386.deb	60811f2afad9261b8af86fd6406125ac

File	MD5
NessusAgent-6.6.2.dmg	6ee0eb28761a349d5ba4a3be0a9eef38
NessusAgent-6.6.2-es5.i386.rpm	ac6ba5ee6a71c7a1cedb296869694366
NessusAgent-6.6.2-es5.x86_64.rpm	b2634a5009f3c5e382887c011bb249b7
NessusAgent-6.6.2-es6.i386.rpm	f42f163d6fb96f725a79089e13bff8b7
NessusAgent-6.6.2-es6.x86_64.rpm	462203313d24d641e25ed0f8fa0387b6
NessusAgent-6.6.2-es7.x86_64.rpm	5f16739dd2201d86ba75f8c2c88eaa0b
NessusAgent-6.6.2-fc20.x86_64.rpm	57d07dd7f58a926ac764408cff7e1da5
NessusAgent-6.6.2-ubuntu1110_amd64.deb	ad9d49f7042ee58795b4bba8243cea1f
NessusAgent-6.6.2-ubuntu1110_i386.deb	26ddb68748cc6b0b0db361a34d2cc0dd
NessusAgent-6.6.2-ubuntu910_amd64.deb	a0eb4ba80a6edfc7ac0b74e95ca5d21f
NessusAgent-6.6.2-ubuntu910_i386.deb	bbc0f2c97bc97679a6b8ebe051967218
NessusAgent-6.6.2-Win32.msi	84ad9dfce6b0a94ca4a5bcc7d3198013
NessusAgent-6.6.2-x64.msi	1323bb1f7375778014e12a072496d54b

Nessus 6.7.0 Release Notes - 5/19/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features / Expanded Platform Support

- Support Thycotic Secret Server as an External Credential Store in Nessus Cloud/Manager
- Allow Nessus to run as a user other than root
- Allow agents and scanners to communicate with Nessus Manager on a different port than the UI
- Nessus Cloud administrators can view scans of all users

Bug Fixes and Improvements

- Simplify linking to Nessus Cloud during scanner set up
- Support OpenJDK for report generation
- Rename "Read-only" user to "Basic"
- Update to OpenSSL 1.0.2h (Security Advisory)
- Allow Nessus to scan by Oracle Clusterware Service Name
- Fixed bug that caused agents to check for updates more frequently than Nessus Cloud instructed them to
- Improve handling of whitespace in target ranges (Nessus Cloud)
- Warn user saves a system asset list with no permissions set (Nessus Cloud)

File Names & MD5 Checksums

File	MD5
Nessus-6.7.0-debian6_amd64.deb	7790483def7fed383b56079dbf47b471
Nessus-6.7.0-debian6_i386.deb	0c1bfd47db49af634e564b73b2a5c431
Nessus-6.7.0.dmg	8e49f38434f8f9b78cd7c88ffc62ba5d
Nessus-6.7.0-es5.i386.rpm	d3a397aa615e2c40529138d1c1aeaa63
Nessus-6.7.0-es5.x86_64.rpm	9de4eea53af76a3d85ba86d7d7655ef0
Nessus-6.7.0-es6.i386.rpm	4938ea3b628d4da76827a5a9b10647bd
Nessus-6.7.0-es6.x86_64.rpm	1065f35f0cc7be2a92b4c2f43d6e5be1
Nessus-6.7.0-es7.x86_64.rpm	d8350a7e0d5e967405d7306261d87dc3
Nessus-6.7.0-fbsd10-amd64.txz	f7d3162110e5956c070617fea75cdfc3
Nessus-6.7.0-fc20.x86_64.rpm	485ab834af50160446e673e6aaf9842b
Nessus-6.7.0-suse10.x86_64.rpm	226225f6a4190b188e3ae9b50bd86384
Nessus-6.7.0-suse11.i586.rpm	2ff3f406cfff35f350c8dec97302560a
Nessus-6.7.0-suse11.x86_64.rpm	6ca538744cb854caf45771701c694c92

File	MD5
Nessus-6.7.0-ubuntu1110_amd64.deb	9e0b3343685ec9bfa22ba6435d36eea3
Nessus-6.7.0-ubuntu1110_i386.deb	2e6333ead2004dd9ab48f55a26ef6db0
Nessus-6.7.0-ubuntu910_amd64.deb	ac48d936dc9ce595c40cd03eb526ce2d
Nessus-6.7.0-ubuntu910_i386.deb	f99d2b2c2ed11d7d280916ca3d5fc691
Nessus-6.7.0-Win32.msi	753f94a74aa5ac484bd085cd92316587
Nessus-6.7.0-x64.msi	1e350064f018a9b87009b58783c5d52d
NessusAgent-6.7.0-amzn.x86_64.rpm	18aee70478967c167807f47fda2e1ac2
NessusAgent-6.7.0-debian6_amd64.deb	56a3e9e2ff5b8dc2aa583b25797f8f0e
NessusAgent-6.7.0-debian6_i386.deb	dc526c78ca2c2fc0453dce13a9530659
NessusAgent-6.7.0.dmg	cae6da00529da4b2228a5326887b0a29
NessusAgent-6.7.0-es5.i386.rpm	b768145c0a6c1697ea878d8fed2f6d95
NessusAgent-6.7.0-es5.x86_64.rpm	c7dec4c053cf3805e359ddc1d8d4e541
NessusAgent-6.7.0-es6.i386.rpm	df58ee402110273dfc6a0501e2a832b2
NessusAgent-6.7.0-es6.x86_64.rpm	5bccd30d2b3f8a04fdaee49ac95884db
NessusAgent-6.7.0-es7.x86_64.rpm	08f6565e743847d0d532a3b192d5f79f
NessusAgent-6.7.0-fc20.x86_64.rpm	03290111d4039c1ff9dd49d9db12f5aa
NessusAgent-6.7.0-ubuntu1110_amd64.deb	65880bb7bf64879b63b1fe0c13acd26b
NessusAgent-6.7.0-ubuntu1110_i386.deb	8461b020d6ad9fab13d226b7880818a7
NessusAgent-6.7.0-ubuntu910_amd64.deb	d432c249ebff01002fde3359e24b56d9
NessusAgent-6.7.0-ubuntu910_i386.deb	7bde8fe2b552c6a1da401085f5c99d8a
NessusAgent-6.7.0-Win32.msi	e2b9e3363f7b3fd7dcc05b4498c7fa20
NessusAgent-6.7.0-x64.msi	1196b1bacfa85c02a71cf2cc7d96e980

Nessus 6.8.0 Release Notes - 7/19/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- Nessus 6.8 includes support for CVSSv3

Bug Fixes and Improvements

- Support for privilege escalation with CyberArk credentials
- Increase file import size beyond 4GB
- Add support for eu-central-1 to AWS cloud audit credentials
- Add support for Yara rules to filesystem malware scanning on Windows
- API docs won't load when trailing slash added to URL
- Uninstall doesn't remove Nessus entries in Start menu on Windows 10
- Agent scans with no results failed to import
- Nessus Certificate information does not contain correct CN (Appliance)
- Imported Nessus DB Scan names have some characters converted to entities
- Prevent policies from being imported via /scans/import
- References to "invalid indexes to hash table"
- nessusd.dump files grows very quickly and may exhaust disk
- Nessus does not properly clean up temporary plugin db files
- Fixed issue with mutex access in logging
- Linking Managed scanners with the same name removes the first scanner
- Update libexpat to 2.2.1 to cover CVE-2016-0718 (Security Advisory)
- Report download should return an error if the report is still being generated
- Results from reverse DNS lookup would overwrite target name if the two were different
- Payload size in the web server log incorrectly reported; for example: -1.

- Plugin 12053 (Host Fully Qualified Domain Name (FQDN) Resolution) claims non-FQDN hostname is an FQDN
- XSS in scan policy drop-down (Security Advisory)
- XSS risk when linking remote scanners in Nessus Manager (Security Advisory)
- Add support in rules processing for hostnames
- Malware policy does not work correctly when using a known bad hash text file
- XSS in User Group name (Security Advisory)

File Names & MD5 Checksums

File	MD5
Nessus-6.8.0-debian6_amd64.deb	04a4f1b605fe85c6407dbc9c1b2ef714
Nessus-6.8.0-debian6_i386.deb	557bc7c9e6ea88d104cab14b0a3b4cf3
Nessus-6.8.0.dmg	11f9f76b86839f8eb899391008af3d4f
Nessus-6.8.0-es5.i386.rpm	45144f12b3cfa636ec29b97bec358705
Nessus-6.8.0-es5.x86_64.rpm	00af63deb00888d056d6a6beb5c0f332
Nessus-6.8.0-es6.i386.rpm	148c0eef3e69ad91b1203ca271d5cf0f
Nessus-6.8.0-es6.x86_64.rpm	0a7bd3986c018690d97d0247562b1c4c
Nessus-6.8.0-es7.x86_64.rpm	2a04fd7b21443f93c17cd3058aa1119f
Nessus-6.8.0-fbsd10-amd64.txz	ce38b62f79202067ec7f81dfecde2dd4
Nessus-6.8.0-fc20.x86_64.rpm	4106308f11c6b56f05932ee7bf9e71e1
Nessus-6.8.0-suse10.x86_64.rpm	f9e7c413f28458e758209578ac08fb66
Nessus-6.8.0-suse11.i586.rpm	e7b3f1b848894e337b39a0b53f4829e9
Nessus-6.8.0-suse11.x86_64.rpm	b97d1b5c78ab68e38d570e3634ee0b3f
Nessus-6.8.0-ubuntu1110_amd64.deb	b856067d3468f816956c8a188aa0a2f1
Nessus-6.8.0-ubuntu1110_i386.deb	c18f563d455baebd52a4d0d41194dd22

File	MD5
Nessus-6.8.0-ubuntu910_amd64.deb	50fe1fae9a6bab2887fc69924e0219c6
Nessus-6.8.0-ubuntu910_i386.deb	47ad8f0740d67bc15cb0d8896d832d6d
Nessus-6.8.0-Win32.msi	e9eff5f4aeee99d4b76bc17c3eb53618
Nessus-6.8.0-x64.msi	499adeee156377ddb63c7a61ee5e927e
NessusAgent-6.8.0-amzn.x86_64.rpm	5fb123d673ccb66157a5594bd756d6eb
NessusAgent-6.8.0-debian6_amd64.deb	4a7bc966810fe77d0128eae9131b44f1
NessusAgent-6.8.0-debian6_i386.deb	7f57d971ed0493fd26345a0c9aa4035f
NessusAgent-6.8.0.dmg	3d887e66610eb334f79fcf3127c8c41f
NessusAgent-6.8.0-es5.i386.rpm	f2ea81875be466850bbfc5948ca31cf7
NessusAgent-6.8.0-es5.x86_64.rpm	d5987727254dc7b673686f3bf9cc4bdb
NessusAgent-6.8.0-es6.i386.rpm	76bddb390e61d1361511e6a6ed9fbec5
NessusAgent-6.8.0-es6.x86_64.rpm	e8ca59176d366ea58c2053d6b45e194e
NessusAgent-6.8.0-es7.x86_64.rpm	089ced49d5cc6972bbdcd805f0882263
NessusAgent-6.8.0-fc20.x86_64.rpm	e8abb60eec745de1712b3b377c4407ae
NessusAgent-6.8.0-ubuntu1110_amd64.deb	41d5e8bd25d54b00cb0d35bc9a0e472e
NessusAgent-6.8.0-ubuntu1110_i386.deb	775543f35365c86294850f39c36b2913
NessusAgent-6.8.0-ubuntu910_amd64.deb	403b59086abec0d3ff9966fe9b791757
NessusAgent-6.8.0-ubuntu910_i386.deb	6c098a300e043ebb96e749e1bc9e2618
NessusAgent-6.8.0-Win32.msi	c917edf9f40919639f42573e5aa0ccc9
NessusAgent-6.8.0-x64.msi	3f9bdf7b2f7eaf48a0b565506a6a28b7

Nessus 6.8.1 Release Notes - 7/25/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Bug in policy configuration may lead to plugins in Settings family not reporting

File Names & MD5 Checksums

File	MD5
Nessus-6.8.1-amzn.x86_64.rpm	2efc851e8e70102c9b89759e97eac086
Nessus-6.8.1-debian6_amd64.deb	7614e1a5fb4d6cb779307b91d7465ed8
Nessus-6.8.1-debian6_i386.deb	e1dd63c0b699c68438c80dd9e052de9d
Nessus-6.8.1.dmg	ab5e7b76f6247592dae5986e0ebf8bf8
Nessus-6.8.1-es5.i386.rpm	d6f2c21ee382477e3eecc808b7e4d965
Nessus-6.8.1-es5.x86_64.rpm	7ce26cc25a3bab50e7a4334afea24fa1
Nessus-6.8.1-es6.i386.rpm	4f48de05a389a7aabf66494acdd2c8fc
Nessus-6.8.1-es6.x86_64.rpm	003b4f239f5cca307f17fc54c94f8d4b
Nessus-6.8.1-es7.x86_64.rpm	491600c672b946b2e4fc68b21df27cb5
Nessus-6.8.1-fbsd10-amd64.txz	bccf3b52bad60deadf4b707138904e98
Nessus-6.8.1-fc20.x86_64.rpm	f697458a7e63fb6915d8e836e128c9bd
Nessus-6.8.1-suse10.x86_64.rpm	d6dd9ccb44eda15ae77b05425aa97ec4
Nessus-6.8.1-suse11.i586.rpm	ef97ac81a23e531d6f4e225e641d2d6e
Nessus-6.8.1-suse11.x86_64.rpm	9c4e92e1c0b810ba0de5e9d4332c1bf2
Nessus-6.8.1-ubuntu1110_amd64.deb	36ac6b925158cdf303973f0e45821bae
Nessus-6.8.1-ubuntu1110_i386.deb	cf01fdd251b6459cc2e7b67f30ecd17c
Nessus-6.8.1-ubuntu910_amd64.deb	390ba66153b1ef988c5ff2bd5e8bf3aa
Nessus-6.8.1-ubuntu910_i386.deb	0274dc3264eda4dab80435418405af76
Nessus-6.8.1-Win32.msi	777ffc938ba0bbf3523d03045a3195e5
Nessus-6.8.1-x64.msi	5f9d5249d4bed4dcdfb46e07cee3b1ed
NessusAgent-6.8.1-amzn.x86_64.rpm	2b87bee5c6cf6e41bac4a29a5e8df954

File	MD5
NessusAgent-6.8.1-debian6_amd64.deb	7c483bc396c5ee2f24bab880f5498dcb
NessusAgent-6.8.1-debian6_i386.deb	a567e30e0b3f069502ef75a21b680a2b
NessusAgent-6.8.1.dmg	8bf1acde0d1f59dcfd4ab87273576c42
NessusAgent-6.8.1-es5.i386.rpm	5d1e891bb61ae6edd7d35d81424e5932
NessusAgent-6.8.1-es5.x86_64.rpm	55b2b0396a08a800c847e550398949c9
NessusAgent-6.8.1-es6.i386.rpm	669b726354859088cbd23e6300227bc8
NessusAgent-6.8.1-es6.x86_64.rpm	0dad46dd5f0cca119bf8bf4e6160ba56
NessusAgent-6.8.1-es7.x86_64.rpm	52898b012fd6cb18c8a7f54cc124828d
NessusAgent-6.8.1-fc20.x86_64.rpm	436f381be101df2e42331b81f4c96775
NessusAgent-6.8.1-ubuntu1110_amd64.deb	aae210e2f7c0df9ef115af1a06d42986
NessusAgent-6.8.1-ubuntu1110_i386.deb	46853f7415994dc8017d9be866a64587
NessusAgent-6.8.1-ubuntu910_amd64.deb	182a46152193b7003ba2c9b93dc2bd15
NessusAgent-6.8.1-ubuntu910_i386.deb	56d281150648f7c303a776031e6fb5d9
NessusAgent-6.8.1-Win32.msi	cf052fea2e911007e714cc69acaf5ed2
NessusAgent-6.8.1-x64.msi	ce9805c61fb3422c8af01db80401e57b

Nessus 6.9.0 Release Notes - 10/25/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features / Expanded Platform Support

- Support for Nessus Professional and Scanners on Kali 2016 Rolling
- Support for Nessus Agents on macOS Sierra
- Support for Nessus Professional and Scanners on macOS Sierra

- Support for Nessus Agents on Windows 2016
- Support for Nessus Pro/Scanner/Manager on Windows 2016

Bug Fixes and Improvements

- Update OpenSSL to 1.0.2j
- Add all 'agent link' command line parameters to installer
- Add toggle to enable/disable malware scan
- Scanner not cleaning up /opt/nessus/var/nessus/users/nessus_ms_agent/reports
- PDF compliance results - long agent names can overlap result output
- Email notification does not display properly in webmail clients
- Uploading an unknown XML file results in a 500, instead of a 400
- Addressed issues with logging
- Scan status says aborted when stopping a running Agent scan.
- Search Agents displays no results when searching for <character>0 in agent name.
- Links are not redirected properly
- getTimezoneOffset is returning the incorrect offset
- It's possible to set the password to an empty string via the API
- Disable export of running scans
- Malware policy does not work correctly when using a known bad hash text file
- Deleting value under "Performance Options" and saving scan will revert to original value
- Clicking on hosts during a running scan can result in "Invalid Hostname" appearing
- Policy download is missing plugin if there are too many individually enabled plugins
- Extra listening sockets are opened on ephemeral ports when remote_listen_port is null
- Edit scan configuration input validation not clearing error when menu was toggled on
- Nessus Manager fails to cleanup broken file upload preventing remote scanners from reuploading scan results

- global.db: Files table not purged where associated scan has been deleted and removed from trash
- Client fails to decode some chunked/gziped packets
- Managed scanners with no user created will fail after application update
- Host IP rather than expected virtual host name is used during web application scan
- Update query for listing scans to fix slow response time
- Improve log rotation
- /etc/machine-id in cloned machines prevents agents from linking

File Names & MD5 Checksums

File	MD5
Nessus-6.9.0-amzn.x86_64.rpm	e07553562b6efb7dbf802d3f05344c6e
Nessus-6.9.0-debian6_amd64.deb	aa5e285c73412fe735afded387a0a6b0
Nessus-6.9.0-debian6_i386.deb	b2eca00745ed02721f61baf4212cfc86
Nessus-6.9.0.dmg	d74a3d05880cfd89e6d5120c4860e81d
Nessus-6.9.0-es5.i386.rpm	98e60caf3bd48f8b97527f97089a66b7
Nessus-6.9.0-es5.x86_64.rpm	2b69a0ffe1e97ba3cb805609365cfd03
Nessus-6.9.0-es6.i386.rpm	6e52bba254af4a28e8fb86fd9c195156
Nessus-6.9.0-es6.x86_64.rpm	936f9bcd4aa66cef1b00666ad8348d53
Nessus-6.9.0-es7.x86_64.rpm	72d94c5ea9aac053524613ba72b8a78f
Nessus-6.9.0-fbsd10-amd64.txz	5dfd6e160e4fd606277c9dcc980a311f
Nessus-6.9.0-fc20.x86_64.rpm	6e18b79673acaa5bc628dde733d739c8
Nessus-6.9.0-suse10.x86_64.rpm	484dc42c62f21515bad2fd1801cbc650
Nessus-6.9.0-suse11.i586.rpm	e8ffe5201206966b4cd6f75e7f3a7f0b
Nessus-6.9.0-suse11.x86_64.rpm	9c923f7d6585c28a5d44c9c670dbc5fc

File	MD5
Nessus-6.9.0-ubuntu1110_amd64.deb	56fc1d7caa410727b783e371a3765b61
Nessus-6.9.0-ubuntu1110_i386.deb	c4786e45818b4d2b5a15acd4d1df2d25
Nessus-6.9.0-ubuntu910_amd64.deb	062e114d0c7df443b87d11784239d6e2
Nessus-6.9.0-ubuntu910_i386.deb	7e23fab5f1a377a11d1aea378e23ff1b
Nessus-6.9.0-Win32.msi	8dcb348e3a2317875cd2891dedc366ae
Nessus-6.9.0-x64.msi	19128ed731d4052fb72d0027b162a6bd
NessusAgent-6.9.0-amzn.x86_64.rpm	501c06c8021be1649c5eb29d8eee85e0
NessusAgent-6.9.0-debian6_amd64.deb	8d77e84ef793ffd39674692eb8ee162a
NessusAgent-6.9.0-debian6_i386.deb	b2b9d4b1ed6872e639ab56f1187102b1
NessusAgent-6.9.0.dmg	43007ec36cfda4a85cdc61dc309e5d2e
NessusAgent-6.9.0-es5.i386.rpm	7d4f6dbc9fe4ac972dc901df63d85be2
NessusAgent-6.9.0-es5.x86_64.rpm	3edb93d5fff788ca022725683251d49d
NessusAgent-6.9.0-es6.i386.rpm	f89429f0eb9f286b22c77ca20608ae8c
NessusAgent-6.9.0-es6.x86_64.rpm	09652dbad3c258e14e2fb1db33cbaea7
NessusAgent-6.9.0-es7.x86_64.rpm	2160d0d1ff5766bbc13061e598b7da73
NessusAgent-6.9.0-fc20.x86_64.rpm	cf62e1901ed03efd79f8a9333c5b75a3
NessusAgent-6.9.0-ubuntu1110_amd64.deb	7d49cc64b357e9f275a5bf98e1fb39b3
NessusAgent-6.9.0-ubuntu1110_i386.deb	2c036b97aa426d6050a710db7ee49a05
NessusAgent-6.9.0-ubuntu910_amd64.deb	ad3222b3802b1c62ca110f90c0c3c42d
NessusAgent-6.9.0-ubuntu910_i386.deb	fd02616d54a3aa1a1d9b7965cc55cb5e
NessusAgent-6.9.0-Win32.msi	06ac2d5c662e60469781ef18d3707ad8
NessusAgent-6.9.0-x64.msi	910a958f060d5b9de26f6f00cf878cf3

Nessus 6.9.1 Release Notes - 11/9/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix a stored XSS vulnerability in policy configuration (Security Advisory)

File Names & MD5 Checksums

File	MD5
Nessus-6.9.1-amzn.x86_64.rpm	54a640dd04b05cc56dc41bd387b7fe87
Nessus-6.9.1-debian6_amd64.deb	270cf98702fd841f9b61a16a6c902765
Nessus-6.9.1-debian6_i386.deb	a4e8446e757bf862d738b22da90a9ed2
Nessus-6.9.1.dmg	83f95a5d96280d44de3b4baf7c8ee6cf
Nessus-6.9.1-es5.i386.rpm	a10d4d805e7b63acb45369e74bff70fc
Nessus-6.9.1-es5.x86_64.rpm	abb4bac6841ee1d74d0da17625911eef
Nessus-6.9.1-es6.i386.rpm	7e00ee218784b71ce2354fd6dcdb87e4
Nessus-6.9.1-es6.x86_64.rpm	fccff91a6c9babbdf8a14874640f0af8
Nessus-6.9.1-es7.x86_64.rpm	0cb9147e28f735a11c0881c582d741fb
Nessus-6.9.1-fbsd10-amd64.txz	c2796c132c7c19bdef4212032f5e46c3
Nessus-6.9.1-fc20.x86_64.rpm	8009fbafb31aa9710fd4113f1094a211
Nessus-6.9.1-suse10.x86_64.rpm	54730add2638caf9beacecd8b7671e97
Nessus-6.9.1-suse11.i586.rpm	e1d68e0db91735097b684880d8cc1cb5
Nessus-6.9.1-suse11.x86_64.rpm	939dbba41194f633fb968db2c6a66323
Nessus-6.9.1-ubuntu1110_amd64.deb	d3fb3a3a8e4cbbca23465daebbdb5fcf
Nessus-6.9.1-ubuntu1110_i386.deb	7dc07e5b437f90977f726e16b92066c7
Nessus-6.9.1-ubuntu910_amd64.deb	0af0d8d75677f7c0f5706b4659045464
Nessus-6.9.1-ubuntu910_i386.deb	9d533aaada049f7778e4f95f0052f8a0

File	MD5
Nessus-6.9.1-Win32.msi	4aa283a206bf5d891315f0625c9133c4
Nessus-6.9.1-x64.msi	f2569c35c5ef50f413802d9546935420
NessusAgent-6.9.1-amzn.x86_64.rpm	2b330c8b8f85d45adbf68a2cc33eb4f3
NessusAgent-6.9.1-debian6_amd64.deb	482e641dc652b8eb2fa9b90700a923fb
NessusAgent-6.9.1-debian6_i386.deb	27e148f58bc0243b9fb0c07d4b685113
NessusAgent-6.9.1.dmg	1cae90d7249ce1af382ed3984b623c63
NessusAgent-6.9.1-es5.i386.rpm	a6e3fe749160ca5feca84e385bd4ad62
NessusAgent-6.9.1-es5.x86_64.rpm	8155bc852ec730e608e5b14493b8c139
NessusAgent-6.9.1-es6.i386.rpm	e9ec34be5192dba7200029d9ff99c6c0
NessusAgent-6.9.1-es6.x86_64.rpm	28a7a505691be120daa405d1427494d8
NessusAgent-6.9.1-es7.x86_64.rpm	6f05fc0dd529c8d8d3800bf46e5e8c50
NessusAgent-6.9.1-fc20.x86_64.rpm	802b0511466075ccbdd53cb26c84349e
NessusAgent-6.9.1-ubuntu1110_amd64.deb	8202550c19c87016d9d8a624e63271fb
NessusAgent-6.9.1-ubuntu1110_i386.deb	0ac4e23463cfef7ad56506473eb95356
NessusAgent-6.9.1-ubuntu910_amd64.deb	6d30860654c15c30d82a2738904a5ce5
NessusAgent-6.9.1-ubuntu910_i386.deb	101178d2ed37adf14620b5a0bb8d8a90
NessusAgent-6.9.1-Win32.msi	9a6e697960977f8f279f4f7850e73fdf
NessusAgent-6.9.1-x64.msi	c6c8c5b85c09e99e762dd97af43159a4

Nessus 6.9.2 Release Notes - 12/14/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix issue adhering to max number of concurrent TCP sessions per scan
- Fix inconsistency in Nessus User Agent version
- Fix memory leak in plugin-code.db agent

File Names & MD5 Checksums

File	MD5
Nessus-6.9.2-amzn.x86_64.rpm	cbb669f91f9f18d3418d15fe9a85f3be
Nessus-6.9.2-debian6_amd64.deb	40d131d53de3902df6bf9332a07a5b53
Nessus-6.9.2-debian6_i386.deb	bb46ec49ae1bae0062fb6275495f47b7
Nessus-6.9.2.dmg	fb39525bfc7f8ef029552dd09fb87478
Nessus-6.9.2-es5.i386.rpm	5a90eaef284cac789b765f35a73d159e
Nessus-6.9.2-es5.x86_64.rpm	ae89de62590136f7cb48fcf4baa41955
Nessus-6.9.2-es6.i386.rpm	d59807b35f398c52966211bd777f2718
Nessus-6.9.2-es6.x86_64.rpm	2fc9038194a21fb35cdc8ebd51dcb1b1
Nessus-6.9.2-es7.x86_64.rpm	994158e493e3e0bdec2ff00cf72d63ed
Nessus-6.9.2-fbsd10-amd64.txz	1a43cb53ece78969847395d36bca0d7a
Nessus-6.9.2-fc20.x86_64.rpm	87a460e111a58a201db0988c6d7a2d54
Nessus-6.9.2-suse10.x86_64.rpm	81905ffbd1a26d87e7fe71b4dd8572b8
Nessus-6.9.2-suse11.i586.rpm	7aa221e7e37738a84b73fd52097dd2f5
Nessus-6.9.2-suse11.x86_64.rpm	387186e9e53784b860fe8e610f9fd1d2
Nessus-6.9.2-ubuntu1110_amd64.deb	dfbc7ab4f60f7d027047224c863e55d4
Nessus-6.9.2-ubuntu1110_i386.deb	0b2e1d46a4461622e5f98b3483d50313
Nessus-6.9.2-ubuntu910_amd64.deb	926207db75b3beb8da5668fb43e64cf8
Nessus-6.9.2-ubuntu910_i386.deb	a5e08906192b4e0e9933601665865cb7
Nessus-6.9.2-Win32.msi	e45d65033e6d4ec57bf4c18268d1a631

File	MD5
Nessus-6.9.2-x64.msi	fa2c6e00c65327245723c18e708f156e
NessusAgent-6.9.2-amzn.x86_64.rpm	284614ca200e3c0b090ff89cf22a71f3
NessusAgent-6.9.2-debian6_amd64.deb	7e3546e58fb812618d1f02d6a23077d4
NessusAgent-6.9.2-debian6_i386.deb	c35961e3fe59c12b181249613a6f733e
NessusAgent-6.9.2.dmg	50788eec63d03b5c37b7e4d5a13789f0
NessusAgent-6.9.2-es5.i386.rpm	647dfb1bc3ed72c42448875a63d8ece1
NessusAgent-6.9.2-es5.x86_64.rpm	3cb27ab7d93d5a805fbb285ddf049b26
NessusAgent-6.9.2-es6.i386.rpm	07ce3fb8059a33cf5b0ee21d8fa7c607
NessusAgent-6.9.2-es6.x86_64.rpm	1633ed2f7960ac01b293f9689a9f5566
NessusAgent-6.9.2-es7.x86_64.rpm	56d95da2f05583121f847bf4f5200a34
NessusAgent-6.9.2-fc20.x86_64.rpm	3e60d48f0d9717547c3a4e10688e878a
NessusAgent-6.9.2-ubuntu1110_amd64.deb	6f47cb87bb50bc841708edbf8cb46203
NessusAgent-6.9.2-ubuntu1110_i386.deb	9ecfc4688aa4c6e188c83dd09d4421aa
NessusAgent-6.9.2-ubuntu910_amd64.deb	a27f73556bc04d6ed26c2d8d79f9602b
NessusAgent-6.9.2-ubuntu910_i386.deb	28875d18c1fce247a6c0e4368fe2e9b4
NessusAgent-6.9.2-Win32.msi	2773df2517532aca57d9a1da9724d1d2
NessusAgent-6.9.2-x64.msi	817c03c031628631f3556187be4672b7

2015 Tenable Nessus

Nessus 6.2.0 Release Notes - 1/20/2015

Nessus 5.2.8 Release Notes - 1/29/2015

Nessus 6.2.1 Release Notes - 1/29/2015

Nessus 6.3.0 Release Notes - 3/3/2015

Nessus 6.3.1 Release Notes - 3/10/2015

Nessus 6.2.0 Release Notes - 1/20/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features, Improvements, Platform Support

- Retrieve an uploaded compliance check audit file
- BlueCoat and Check Point compliance wizard updates

- Add package reporting for Red Hat Enterprise Linux and SuSE Linux to Altiris PM integration
- Ability to Disable Scheduled Scans
- Credential and Compliance search
- Improved notifications UI
- Nessus 6 available for i386 (32-bit) architectures
- OS X 10.10 (Yosemite) support
- Fedora 21 support

Bug Fixes

- Incomplete log message when stopping a scan
- Bug Report Generator Issues
- Double upload requests when manually uploading files
- Incorrect restart reason can show up in logs
- Bogus scan range causes scanner to scan non-specified targets
- mkdir crashes on Windows
- Sorting after search sorts on full data set
- Scan history is not being purged when scan is deleted
- Mixed plugin families are not saved correctly when filtering is used
- Modal Window hangs after deleting a subset of policies
- Some remote scans are aborted if being started just before a reload of the manager
- nessuscli fetch --code-in-use writes to the root directory instead of the tmp directory
- 6.0.X won't automatically update to 6.1.2 on Windows
- Race condition can allow scanner to set a "done" job back to "completed" and attempt re-processing
- CentOS RPM depends on KILLALL being installed, which is not a default package in the CentOS7 minimal install

- Multiscanner use proxy checkbox is not enabling proxy functionality with secondary scanners
- Attachments in scan results cannot be downloaded
- Make bug report generator help text clearer
- Upgrading via MSI makes Nessus unable to be uninstalled or upgraded
- FortiGate Best Pract check: Error 500 creating advanced policy in both advanced and offline config wizard
- Various API errors reported on support forums

Note:

- There is now one user guide for Nessus and Nessus Enterprise.

File Names & MD5 Checksums

File	MD5
Nessus-6.2.0-debian6_amd64.deb	09465c65d7ed80a0853b8ebc9f2c0aa0
Nessus-6.2.0-debian6_i386.deb	65d458d0c1c7d8aad0d2b93b40a487ac
Nessus-6.2.0.dmg.gz	8e1dd9ff9212cd37771a1bdb088492ce
Nessus-6.2.0-es5.i386.rpm	20b63461c79a14e4408a8af8fe87b8c8
Nessus-6.2.0-es5.x86_64.rpm	b9fcf6dc0dc23f4f652ac55a3450a340
Nessus-6.2.0-es6.i386.rpm	fe14949b31c16fe22681d7125483cd50
Nessus-6.2.0-es6.x86_64.rpm	4f5c5c846b691b5198d54436ab03ca86
Nessus-6.2.0-es7.x86_64.rpm	a548ef591d7040bf577d91d69e1f42cb
Nessus-6.2.0-fbsd10-amd64.txz	f2c81422dcad9cda4476960ba848a86b
Nessus-6.2.0-fc20.x86_64.rpm	9c9d19d4c207254455c779c3f4a3f4dc
Nessus-6.2.0-suse10.x86_64.rpm	c12d56dade0fc1224f85448a1146468f
Nessus-6.2.0-suse11.i586.rpm	2fdde2b42260fee35e776ffb1c50f8e6
Nessus-6.2.0-suse11.x86_64.rpm	ac5b0b4b174e7cafc7003f2548d0a092

File	MD5
Nessus-6.2.0-ubuntu1110_amd64.deb	d6e4740c5676ad3a78d5881b65e9a9b2
Nessus-6.2.0-ubuntu1110_i386.deb	f445104c57b5662cc3a69fd72c103c2d
Nessus-6.2.0-ubuntu910_amd64.deb	e162cbb3a89782157cafcd30b45e11dc
Nessus-6.2.0-ubuntu910_i386.deb	49e15b38a9b3179956642bde6c02870c
Nessus-6.2.0-Win32.msi	528478e8681fbdc6f0ddbd7a5dd7edd4
Nessus-6.2.0-x64.msi	a0443fa58f719045b76955c11fe0e4cc

Nessus 5.2.8 Release Notes - 1/29/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Scans return with "No host data" after a plugin update

File Names & MD5 Checksums

File	MD5
Nessus-5.2.8-debian6_amd64.deb	638e3d9e757766f8429f2a8691c09af6
Nessus-5.2.8-debian6_i386.deb	adb9fc972c17b7a5f6f499f7279056ab
Nessus-5.2.8.dmg.gz	74896f2e235789729b3a075fa1ea8ae1
Nessus-5.2.8-es4.i386.rpm	4679ef3e2c0c75995b34b9d0f96c7025
Nessus-5.2.8-es5.i386.rpm	3a2ccbced9d249262ae5d8d53c45e807
Nessus-5.2.8-es5.x86_64.rpm	bd04856832c160d3b61558e8a9a80a42
Nessus-5.2.8-es6.i386.rpm	cdc92cd933e27cc43e57dda703ef5ba7
Nessus-5.2.8-es6.x86_64.rpm	0fa42b7e3ec68f7d29be2637a2dd4c8e
Nessus-5.2.8-fbsd9-amd64.tbz	3fb19cf5f6742aeb188a029ffe352ac5

File	MD5
Nessus-5.2.8-fbsd9.tbz	a5125a379a4034a24a198a4af9288b0a
Nessus-5.2.8-fc16.i386.rpm	48d32ead4b4459ff7ffc06b7228c3a97
Nessus-5.2.8-fc16.x86_64.rpm	9abaa4c0bab522ea0e10893c326441ff
Nessus-5.2.8-suse10.x86_64.rpm	864ba6514d898417cee2fed4160ceb85
Nessus-5.2.8-suse11.i586.rpm	3259f16784ab764b6909fc6db0d70214
Nessus-5.2.8-suse11.x86_64.rpm	c161b99f18830f6e8d6517bdeb142757
Nessus-5.2.8-ubuntu1110_amd64.deb	0d114fda16cf7d5120310b904182ac22
Nessus-5.2.8-ubuntu1110_i386.deb	9954005c13568db20386e7f9119bb2eb
Nessus-5.2.8-ubuntu910_amd64.deb	e90214388af92e81c8ce11d328d5abde
Nessus-5.2.8-ubuntu910_i386.deb	a3825aa7afe38fd3f824ecec15b3bd10
Nessus-5.2.8-Win32.msi	70de46cc8bccbc712389757a22c7c832
Nessus-5.2.8-Win32_XP2K3.msi	b5e718ed7c0539c32878e4058d793081
Nessus-5.2.8-x64.msi	f6003cfb5a8c53b79506dbca2e3ee41c
Nessus-5.2.8-x64_XP2K3.msi	d1f8d74bf847f3e91bc07f7c06da7b2a

Nessus 6.2.1 Release Notes - 1/29/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Scans return with "No host data" after a plugin update
- Blue Coat is missing from the compliance UI
- Scheduled Jobs are not running, with no indication of failure or why they didn't run

File Names & MD5 Checksums

File	MD5
Nessus-6.2.1-debian6_amd64.deb	96d284b5a3d321af1181fa86a94788fe
Nessus-6.2.1-debian6_i386.deb	c0a96029e6f399e4ab25e7bbf93f1f72
Nessus-6.2.1.dmg.gz	05cae3b0efc5032a0f01b8d18579ac73
Nessus-6.2.1-es5.i386.rpm	7f9e6c2d4f28aef08d7c0dc5b40d4a82
Nessus-6.2.1-es5.x86_64.rpm	0d7076b9de55ae3ea3ddf4e2b3faf2c7
Nessus-6.2.1-es6.i386.rpm	f0c2c0a074e07aac309e1b85732abb22
Nessus-6.2.1-es6.x86_64.rpm	c58cf80fe59514902cb880af88a4b1a9
Nessus-6.2.1-es7.x86_64.rpm	48a2595a9be6fabfbb899a03a4327aaa
Nessus-6.2.1-fbsd10-amd64.txz	b1db7e4d937114eb96fc9765849254d9
Nessus-6.2.1-fc20.x86_64.rpm	254f1a37e7cc560df149c3cb1277d869
Nessus-6.2.1-suse10.x86_64.rpm	77779b8950d01b6c9f1049e811911f72
Nessus-6.2.1-suse11.i586.rpm	e0f436c55f2530833d618a5e80c936b8
Nessus-6.2.1-suse11.x86_64.rpm	2276b5ab3bbb337d08e3e6abd8686ce7
Nessus-6.2.1-ubuntu1110_amd64.deb	eb5c92819d8bdba3a522aa6c33c7d473
Nessus-6.2.1-ubuntu1110_i386.deb	1f0927b6221064492a4a9a3f9ee8ebe1
Nessus-6.2.1-ubuntu910_amd64.deb	05b8db2c1f4d7a9341bc3bc9f993f19b
Nessus-6.2.1-ubuntu910_i386.deb	c2fda984715d5dd438e439625e8624ba
Nessus-6.2.1-Win32.msi	4d10fe9f28cfd1b8a8197dd3ae51c9d0
Nessus-6.2.1-x64.msi	1ae73b89adbd0f9f50a938cc4185668b

Nessus 6.3.0 Release Notes - 3/3/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features, Improvements, Platform Support

- Nessus Agents for Windows
- Scan Dashboards
- Only use responsive layout on mobile devices
- Add the ability to disable/enable scans from the scan list
- New Licensing Model
- Scan multiple DB instances in single compliance scan

Bug Fixes

- nessusmgt can crash when run with no arguments
- Filtering plugins to disable 1 plugin disables entire family
- Files for active SCAP components do not download from policy editor
- Autoupdates that require soft restart don't work as expected
- Running a diff on a scan requires edit access due to lack of ability to select scans with read only.
- API: Creating a job with improperly formated RRULES json property causes job to become corrupt and folder inaccessible.
- VMware compliance scans don't work from Compliance Wizard, work fine from advanced option
- Modified time format in Scans/Policy screen is 24 hour time w/ PM indicator
- Windows Installer does not install plugins-core, or installs it to the wrong place
- Undefined host in /scans/XX/hosts/undefined/plugins/YY produces 404
- Vulns list auto-scrolls back up
- Network Port Scanner: Overriding Firewall Detection defaults from TCP will clear enabled override type from SYN, and vice versa
- When uploading scan results, the results go into "My Scans" regardless of the folder selected.
- Test for /nessus6-api.html#/resources/scans/launch incorrectly encodes alt_targets
- Changing the custom host does not restart the webserver

Known Issues

- SecurityCenter-managed Nessus 6.3 scanners currently do not have have full policy and scan capability; this will be addressed in an upcoming release. It is not advised to install or upgrade Nessus scanners managed by SecurityCenter to Nessus 6.3.

File Names & MD5 Checksums

File	MD5
Nessus-6.3.0-Win32.msi	01321c1d7e315e091e26ed039abcc0ac
Nessus-6.3.0-debian6_amd64.deb	523eedc53e7353361d1a0782a313fdf0
Nessus-6.3.0-debian6_i386.deb	1ed97143feffb53d4d1bfeadc44ac68b
Nessus-6.3.0-es5.i386.rpm	9bac97cd7010d808d9f1dd25a2f98ee2
Nessus-6.3.0-es5.x86_64.rpm	69a3c16655de98d259673fd870a04cd8
Nessus-6.3.0-es6.i386.rpm	20d6a96f36c6ea16f893b4db34aa80d5
Nessus-6.3.0-es6.x86_64.rpm	eaaa5607ab9af89ebb840e73db025080
Nessus-6.3.0-es7.x86_64.rpm	a3921c58a43ea9e99a65a867c2574f09
Nessus-6.3.0-fbsd10-amd64.txz	f753cb2d513f3d94a990ec7237e0f68f
Nessus-6.3.0-fc20.x86_64.rpm	02b17442a7f18a0d9a7d10ebf71e0a7c
Nessus-6.3.0-suse10.x86_64.rpm	275dee27a6ccc408ff7e84b88c11495e
Nessus-6.3.0-suse11.i586.rpm	647d3b2f8652b7ca97a928925f4a1a06
Nessus-6.3.0-suse11.x86_64.rpm	7c4aaf4dabd819c82e1bc7cb30115fd1
Nessus-6.3.0-ubuntu1110_amd64.deb	424e7f9ffe988f5617b9933dcf11d0f2
Nessus-6.3.0-ubuntu1110_i386.deb	7523c5449651c2ef0774e593bfe256aa
Nessus-6.3.0-ubuntu910_amd64.deb	ded218f31e5490b6214484530d636352
Nessus-6.3.0-ubuntu910_i386.deb	3be72f0dd45f9a0d594ce2253639cdb0
Nessus-6.3.0-x64.msi	414c70a3c6b84caeaf101b793aa36b2b

File	MD5
Nessus-6.3.0.dmg.gz	d44803efce3fb46cac87e04ec78cc71e
NessusAgent-6.3.0-Win32.msi	10793acbffb3bab1c6598efccdebab03
NessusAgent-6.3.0-x64.msi	b400fe20a2b29f568cdfb83f1038465d

Nessus 6.3.1 Release Notes - 3/10/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Write errors in the logs
- Canceling out of changing your password goes to scans
- web server binds on 0.0.0.0 instead of listen_address
- Some Nessus Home installation are stuck in "Unknown mode" after upgrade
- Web server (6.3) not accessible with some network interface configurations
- No Scanner Found when upgrading an unregistered scanner from 6 to 6.3
- Incorrect logging of the local address
- UI not refreshing for group functions and removing secondaries in IE 11 (9 and 10 as well)
- During initial setup, all wizards display "Welcome to Nessus" as the tag for the page
- Issue with agent groups not appearing after creation in IE 11
- Upgrade using 6.3 msi from 5.2.8 causes error during install 1920 "failed to start"
- Registering Nessus 6.3 in IE returns to the welcome screen
- SecurityCenter-managed scanners should have full scan and policy capability

File Names & MD5 Checksums

File	MD5
Nessus-6.3.1-Win32.msi	6350f1e468e5aca87c8a4bae1990b719

File	MD5
Nessus-6.3.1-debian6_amd64.deb	184fe44e63e4f25e7e3b3bd65f35c4d1
Nessus-6.3.1-debian6_i386.deb	401179ab6e03f276300188ae8e81064d
Nessus-6.3.1-es5.i386.rpm	b858d57c8746a9d0dc5dbb0551594ec2
Nessus-6.3.1-es5.x86_64.rpm	1faf66fc0ab0dd3ee59aaba11b7cf1c8
Nessus-6.3.1-es6.i386.rpm	e49d6e1f2d2990e35e33e484c788b9f5
Nessus-6.3.1-es6.x86_64.rpm	13455190a6922788d734427ba2a2ed41
Nessus-6.3.1-es7.x86_64.rpm	fd6fdda2e0f77a4606bffa9aae044e9d
Nessus-6.3.1-fbsd10-amd64.txz	b48e4016e2bf5af9319c64c4cfe9b665
Nessus-6.3.1-fc20.x86_64.rpm	5c7b1f5ce98b1624a623bf2055dc2ad4
Nessus-6.3.1-suse10.x86_64.rpm	9f7fb9177e59f93bceda847d283f5d85
Nessus-6.3.1-suse11.i586.rpm	f4106dccfaf0b685b5750cc36c2ff02a
Nessus-6.3.1-suse11.x86_64.rpm	3d8219b7db62fc0f6d41f2c97a2bc356
Nessus-6.3.1-ubuntu1110_amd64.deb	cdb5b0402c1a1ac1c5bea12737b93662
Nessus-6.3.1-ubuntu1110_i386.deb	c8997b19eb944e3fb4d037843865f116
Nessus-6.3.1-ubuntu910_amd64.deb	324f16ad7709f28769268ead7f6a501c
Nessus-6.3.1-ubuntu910_i386.deb	4575a54e8339e5e82e8dc7c9b58e8a26
Nessus-6.3.1-x64.msi	aca69ae21fd36a824fae78ed6c8e8f23
Nessus-6.3.1.dmg.gz	94461d90a4a594943068165f2d6dff7d
NessusAgent-6.3.1-Win32.msi	704c0170c221e5360e4ce2c3828dd9bf
NessusAgent-6.3.1-x64.msi	71ac8cdd5d65e4aac3a962a48ea476da

Nessus 6.3.2 Release Notes - 3/11/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Customers who are running 6.3.0 or 6.3.1 (this does not apply to agents) will need to manually upgrade by downloading the installation package for 6.3.2 and following the appropriate steps to upgrade as outlined in the Nessus 6.3 Installation and Configuration Guide.

Bug Fixes

- Attempts to upgrade to 6.3.1 fail with "Could not validate preference" in logs and require a reset of the activation code

File Names & MD5 Checksums

File	MD5
Nessus-6.3.2-Win32.msi	b3be9bf8c7d41304023605cf6910b1ca
Nessus-6.3.2-debian6_amd64.deb	1f4cd5b0991ff69f3ca839cd8d76247b
Nessus-6.3.2-debian6_i386.deb	591c1a2b3541a6299f4762804b924209
Nessus-6.3.2-es5.i386.rpm	f714ded33439c9fe18a7ebd55290493e
Nessus-6.3.2-es5.x86_64.rpm	7f9a8d8f15cd6948cffd36908db67bca
Nessus-6.3.2-es6.i386.rpm	c0e9ceb5fe352fc0f2f33f5f7ad55fa5
Nessus-6.3.2-es6.x86_64.rpm	e34c61c2925da50f70774b79f32c7d8a
Nessus-6.3.2-es7.x86_64.rpm	f6a63324665a0fb703b009cbd48daded
Nessus-6.3.2-fbsd10-amd64.txz	743dad8239970ea14cc17006797a5f15
Nessus-6.3.2-fc20.x86_64.rpm	4c676965ec8d1e131ad03dbec82f492a
Nessus-6.3.2-suse10.x86_64.rpm	b3c6a106b4d731c3e17e89bc0ec439aa
Nessus-6.3.2-suse11.i586.rpm	64f71f05fdb74b8e5ad53afd51637146
Nessus-6.3.2-suse11.x86_64.rpm	45b3158d4d7398be3c94362886f65c77
Nessus-6.3.2-ubuntu1110_amd64.deb	1f6548bea0be75db38e2f328d3649671
Nessus-6.3.2-ubuntu1110_i386.deb	2553bea4b3beee1aa8d84f6e6c82e3b8
Nessus-6.3.2-ubuntu910_amd64.deb	36337ef8754bfd04c43c5a527373b1b6
Nessus-6.3.2-ubuntu910_i386.deb	9af1424d3179e4415f14aee0e084ff03

File	MD5
Nessus-6.3.2-x64.msi	632c7b2bda2fa553949828c6ec3b9d71
Nessus-6.3.2.dmg.gz	7bde56bdab46f398c853f3f2d74a09ba
NessusAgent-6.3.2-Win32.msi	a99f4e211f75134b3981730cc520575f
NessusAgent-6.3.2-x64.msi	8157f01f46dc602f4397cb6db167acae

Nessus 6.3.3 Release Notes - 3/16/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Airwatch - Unable to scan via GUI
- Possible deadlock condition on manager if plugins-attributes.db is corrupted.
- offline update fails with current plugin file (all-2.0.tar.gz)
- Bug report email address no longer exists
- Command Line Output for Offline Registration Uses Wrong URL for Nessus 6.3+
- Master password does not work through GUI
- Remote scan job reference is not saved on reload
- Manager: autoupdates fork aborts during update
- Dashboard file is not deleted on disk when scan is removed
- Agent plugin output displaying incorrect data

File Names & MD5 Checksums

File	MD5
Nessus-6.3.3-Win32.msi	14ac975bddfa2bb109cdcf3eaa9fee51
Nessus-6.3.3-debian6_amd64.deb	62fc30b057effb0979f4117f2e7d9630
Nessus-6.3.3-debian6_i386.deb	2381ac1bc203e51c97cc3bd47d9ee2c7

File	MD5
Nessus-6.3.3-es5.i386.rpm	d67fb504e3a04b48463bb494222cc698
Nessus-6.3.3-es5.x86_64.rpm	db27ebfd25c0a04c1a50fc1d7db0e199
Nessus-6.3.3-es6.i386.rpm	a9297adc79edf4a9675b8ae2125830e1
Nessus-6.3.3-es6.x86_64.rpm	fd15b89a926c38e24fb21ff7d37cabac
Nessus-6.3.3-es7.x86_64.rpm	1412a3aa33d4df84582256d2ba0370e9
Nessus-6.3.3-fbsd10-amd64.txz	29eadd9b1f573e12b9e454795133c8c0
Nessus-6.3.3-fc20.x86_64.rpm	410d1e8e41506368bf9e637d6b986226
Nessus-6.3.3-suse10.x86_64.rpm	2d1ff86347441f4cca5d346a4e59a7dd
Nessus-6.3.3-suse11.i586.rpm	9266ead81da7f6aa871fc458addf56c8
Nessus-6.3.3-suse11.x86_64.rpm	77c6c5b7ff1cfe7019209aa25d3e8e8b
Nessus-6.3.3-ubuntu1110_amd64.deb	b04bc424a66a2a081a83da6be8cef01c
Nessus-6.3.3-ubuntu1110_i386.deb	2422051e0ca8d8bf02fd9662c104d7d0
Nessus-6.3.3-ubuntu910_amd64.deb	22c0d0728116a9bbd710defe272525c7
Nessus-6.3.3-ubuntu910_i386.deb	4ae9ac2d9f7dff36b8ed498d40138039
Nessus-6.3.3-x64.msi	b4ce251264d4cfbee7cbff623d5b468f
Nessus-6.3.3.dmg.gz	8934e32238a0ef4ff62b9243a668f87c
NessusAgent-6.3.3-Win32.msi	70c8853a3389f2c814e4dbae99563208
NessusAgent-6.3.3-x64.msi	54d689895df9f93fb021af5f602b8f82

Nessus 5.2.9 Release Notes - 3/30/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Update OpenSSL to 1.0.0r (See Security Advisory)
- Nessus is not freeing gzip memory on HTTP session end

File Names & MD5 Checksums

File	MD5
Nessus-5.2.9-debian6_amd64.deb	397a6ad5d5786594b988e44ad5d8587d
Nessus-5.2.9-debian6_i386.deb	819531e8873609ce57a987badbe69613
Nessus-5.2.9.dmg.gz	09af0812a75e4b58007858ca4f0d4f8d
Nessus-5.2.9-es4.i386.rpm	d69334ae0d8d1aaacb66a0ee66587b9e
Nessus-5.2.9-es5.i386.rpm	318d2348ea7d6a4fba296f0030465a75
Nessus-5.2.9-es5.x86_64.rpm	41dd89c174f86c014e9e75cab6b94112
Nessus-5.2.9-es6.i386.rpm	392e73b1d509af1f57eac37da057894e
Nessus-5.2.9-es6.x86_64.rpm	296ceb927e83231f6d7704e7cbbc8559
Nessus-5.2.9-fbsd9-amd64.tbz	c4b89906eb25854f82ef28da89d20257
Nessus-5.2.9-fbsd9.tbz	6bbc92a4d5c2a702535861ea13787ad9
Nessus-5.2.9-fc16.i386.rpm	781d9855352e227374ecff2f1e27596a
Nessus-5.2.9-fc16.x86_64.rpm	8434526c20f08fb09348ec5b7a19b878
Nessus-5.2.9-suse10.x86_64.rpm	1a70fe0624b099fb7d635561a7f76428
Nessus-5.2.9-suse11.i586.rpm	bfddccd2779c143d005f5674aab7e3f7
Nessus-5.2.9-suse11.x86_64.rpm	6dd6f06ea286f1e7206d4e50260cf8d1
Nessus-5.2.9-ubuntu1110_amd64.deb	c9411504b219d12436ff53d05af4a71e
Nessus-5.2.9-ubuntu1110_i386.deb	7c13a745d245109899bf6339852e2aee
Nessus-5.2.9-ubuntu910_amd64.deb	89a478960e6f4598c13d8ed0a41c9ab8
Nessus-5.2.9-ubuntu910_i386.deb	93417217fb764bab59bd7a87df3d1a45
Nessus-5.2.9-Win32.msi	a2b4208d9992779ed47ec378b460d031

File	MD5
Nessus-5.2.9-x64.msi	fd37a8ab63f219eed190a937e2e693dd

Nessus 6.3.4 Release Notes - 3/30/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Update Debian package descriptions to remove references to Nessus version
- Remote Scanner plugin tar file is not generating correctly on Centos 7
- Nessus installer fails on Debian when upgrading existing install
- Update OpenSSL to 1.0.0r (See Security Advisory)
- Agent scans are showing duplicate entries in Reference Information under Plugin Details
- Host detail information is only present for one agent in a multiple agent scan
- Searching through the agent lists displays a perpetual loading spinner
- Agent results are not reporting correctly when multiple agent scans are running
- Users can not stop Agent scans
- In settings/port scan, netscan(wmi) is listed twice.
- Nessus is not freeing gzip memory once an http session is over

File Names & MD5 Checksums

File	MD5
Nessus-6.3.4-debian6_amd64.deb	cc29bb0c8696a0e5644fd548017dcd31
Nessus-6.3.4-debian6_i386.deb	f768155141d1857505586467b911040b
Nessus-6.3.4.dmg.gz	b973e2f365ef226a5f0c3a39aa0c1612
Nessus-6.3.4-es5.i386.rpm	3fcf7a052dfc1ac5ebfca579096089ae
Nessus-6.3.4-es5.x86_64.rpm	b3bad38c80b6ab74af551c205793d54b

File	MD5
Nessus-6.3.4-es6.i386.rpm	0fd85396577131865515704509d1c378
Nessus-6.3.4-es6.x86_64.rpm	6edb900642d569a904cf3a6787afbbd7
Nessus-6.3.4-es7.x86_64.rpm	1207074ccdb8dedd84400e5336b62faf
Nessus-6.3.4-fbsd10-amd64.txz	b1935f05ede92dfbce7ea55ce6e37ac1
Nessus-6.3.4-fc20.x86_64.rpm	4a0ee390c09cde5529c4d1fdf301042c
Nessus-6.3.4-suse10.x86_64.rpm	de759f34f750d030c3400a8090f1c7a5
Nessus-6.3.4-suse11.i586.rpm	e00170822685461a1750007d82ae91a3
Nessus-6.3.4-suse11.x86_64.rpm	db43de8b4ca959bca4db3ed1571afe25
Nessus-6.3.4-ubuntu1110_amd64.deb	4da473613c4900e9435cf033b31cd61c
Nessus-6.3.4-ubuntu1110_i386.deb	aa5200d226292a80b7ddc4ba76d952fe
Nessus-6.3.4-ubuntu910_amd64.deb	905831db7c3105be8fe9da80288a1eba
Nessus-6.3.4-ubuntu910_i386.deb	c2f6a074e4569f12d94556f5545e0f94
Nessus-6.3.4-Win32.msi	9c44dfcb32c12a6c2739093c1eb6a73f
Nessus-6.3.4-x64.msi	93411bf6124e30f6905ea92d1f6e4edd
NessusAgent-6.3.4-Win32.msi	2dceb53ff9eb371387b61ba35a57bdc3
NessusAgent-6.3.4-x64.msi	d4cc63ae021039ae6025f5b77b84fb3e

Nessus 6.3.5 Release Notes - 4/22/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- SC policies are not always removed from policies.db
- Update Cisco ISE connector text to reflect compatibility with ISE 1.2
- Proxy requests are duplicating the port when fetching updates

- Unix Compliance audit files listed under Windows on 32 bit platforms
- Seeing "function call from non-address variable" in the nessusd.dump in US-1A
- Agent scans might not execute due to an incorrect IP address
- Scanner job list will append running jobs over and over on update
- When scanner (old or new) registers, the scanner cannot be deleted until Nessus is restarted
- Unlinking an agent does not remove the agent from the manager if the web service was not reloaded
- If a user clicks "re-key", the newly generated key cannot be used to link a scanner or an agent until the Nessus instance is restarted
- Sleep time too short on agent - seeing warnings in log
- Issue continuing agent scan after reloading with multiple scans in queue
- Disabling one plugin, disables all plugins in family, family status says "mixed" on 32 bit OS only

File Names & MD5 Checksums

File	MD5
Nessus-6.3.5-debian6_amd64.deb	256b445d0b3a7bbd5b11978e3025b772
Nessus-6.3.5-debian6_i386.deb	5bd389ce6540f81ee636e91912c53ee4
Nessus-6.3.5.dmg.gz	f6a4efacc5cf9ebd32ff41d6e016b3fa
Nessus-6.3.5-es5.i386.rpm	94d638c315c6869d3b5828f32e210764
Nessus-6.3.5-es5.x86_64.rpm	98d93e9a8e917ca20030dfc014d36f6f
Nessus-6.3.5-es6.i386.rpm	79fef137257d6336be2eab645d166586
Nessus-6.3.5-es6.x86_64.rpm	3025f75bfc6e6e3dfe8f0dd8f92b3242
Nessus-6.3.5-es7.x86_64.rpm	9a9c3f9e7725db61ec4af75df52c374c
Nessus-6.3.5-fbsd10-amd64.txz	a5efb86db7ffe6f2d1ba7b24cae5cbc9
Nessus-6.3.5-fc20.x86_64.rpm	a33fe5ddcfdeafc5a549bcfb5c75f7f6
Nessus-6.3.5-suse10.x86_64.rpm	5ba66d6307e2380755e5271eb52c0c74

File	MD5
Nessus-6.3.5-suse11.i586.rpm	27e29731b5be124ffeeef5989ab5bc70
Nessus-6.3.5-suse11.x86_64.rpm	e4813e74e8a8adbbf94e82bcba87fcbd
Nessus-6.3.5-ubuntu1110_amd64.deb	7620eeb152abfc132cd28780c240cc90
Nessus-6.3.5-ubuntu1110_i386.deb	f696763b4491bdfde2d4aee5223f08b9
Nessus-6.3.5-ubuntu910_amd64.deb	0f4b1cb4a50f052481734ae790d82ae7
Nessus-6.3.5-ubuntu910_i386.deb	84d511eac3a3fb62d1b5264ca289865f
Nessus-6.3.5-Win32.msi	a67dfe461d28c284ae6cc9c53717ff54
Nessus-6.3.5-x64.msi	f17b31548d97dc04eabed2a6b1896895
NessusAgent-6.3.5-Win32.msi	3349b54464d7b9ead5434fcef3a5fae3
NessusAgent-6.3.5-x64.msi	90fbb392b773936e53bb4fd71e1a8c7d

Nessus 5.2.10 Release Notes - 5/6/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Scans started from SecurityCenter may experience degraded performance

File Names & MD5 Checksums

File	MD5
Nessus-5.2.10-debian6_amd64.deb	697c690e6365147fe003f871e505bd16
Nessus-5.2.10-debian6_i386.deb	838e982d1404816510f43c6f90b4d37b
Nessus-5.2.10.dmg.gz	957053da71150e9e42f8a60b782cc79f
Nessus-5.2.10-es4.i386.rpm	3ef432d57d04d5def5dbc62a23eda9db
Nessus-5.2.10-es5.i386.rpm	bf4734787cf287967f19031573b10c5d

File	MD5
Nessus-5.2.10-es5.x86_64.rpm	a6e2d431ec0b14df4e51321285b3153c
Nessus-5.2.10-es6.i386.rpm	9e90df43d4c642c8ea719c00479f6234
Nessus-5.2.10-es6.x86_64.rpm	7855d98624b8b5a3caa6db4743e9c66b
Nessus-5.2.10-fbsd9-amd64.tbz	374606f5b05c30fbb72b6f646babfb2a
Nessus-5.2.10-fbsd9.tbz	5ff7ee6dd6320cc904d477cb6c8cd93d
Nessus-5.2.10-fc16.i386.rpm	6991b7d8d4236991d2ca0ff101393189
Nessus-5.2.10-fc16.x86_64.rpm	699aedb943790d1637bb185a858bd821
Nessus-5.2.10-suse10.x86_64.rpm	8c18a66b6dcb79eb0522b0e16606392c
Nessus-5.2.10-suse11.i586.rpm	d9849a94bec1e0886e631acaf8ceb7b7
Nessus-5.2.10-suse11.x86_64.rpm	f5c4d0c6dc2960541f6bd0a448408273
Nessus-5.2.10-ubuntu1110_amd64.deb	7c897dd8f9b0d568c66509ccd76673e4
Nessus-5.2.10-ubuntu1110_i386.deb	9b726869ad1686c2400323d1ad2b3ce0
Nessus-5.2.10-ubuntu910_amd64.deb	6e2a78d75376a918404dd483ca28233f
Nessus-5.2.10-ubuntu910_i386.deb	3e14db4bd9a5a0d26d21167e09dc4923
Nessus-5.2.10-Win32.msi	cf288988dac2f0d9f3ffbbceecdeee5f
Nessus-5.2.10-x64.msi	a32235aaf5107d11f34f520c9d58a054

Nessus 6.3.6 Release Notes - 5/6/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Scans started from SecurityCenter may experience degraded performance

File Names & MD5 Checksums

File	MD5
Nessus-6.3.6-debian6_amd64.deb	598c48e92c507010277fba490e943fca
Nessus-6.3.6-debian6_i386.deb	cca32de4eec9f66d6cc5ea595b7062e2
Nessus-6.3.6.dmg.gz	a6b96c166c3dece383ebda3a9735a989
Nessus-6.3.6-es5.i386.rpm	2c8816a61500c0650df36b4551bb22a3
Nessus-6.3.6-es5.x86_64.rpm	40a46e118f2027fa87a9e6ca277c6273
Nessus-6.3.6-es6.i386.rpm	24af58c88e85f632d6bc6103ab6c5813
Nessus-6.3.6-es6.x86_64.rpm	8cf465f615d95a768b62891500f62242
Nessus-6.3.6-es7.x86_64.rpm	98d09bea814bb8a270eb29eb96f7b522
Nessus-6.3.6-fbsd10-amd64.txz	6500daceac35a41ef06c144bae6a7b5c
Nessus-6.3.6-fc20.x86_64.rpm	5242b99e44bcdfa00d2e79afd2cb51fd
Nessus-6.3.6-suse10.x86_64.rpm	380fb84da855ecd0d6e2434d67bcb21c
Nessus-6.3.6-suse11.i586.rpm	7bb53a71b6c9ed790a084e8318a11e77
Nessus-6.3.6-suse11.x86_64.rpm	c36003e69145ce06647927b20a634b16
Nessus-6.3.6-ubuntu1110_amd64.deb	777fc3bbb81f816dbbbba2209a51f56f
Nessus-6.3.6-ubuntu1110_i386.deb	6647c36672b866a2ad4e875ab068730e
Nessus-6.3.6-ubuntu910_amd64.deb	3a4c96daeeed114d5a3225ddb207d4f9
Nessus-6.3.6-ubuntu910_i386.deb	44bef1d0f2309b2da03d6c34a4f17509
Nessus-6.3.6-Win32.msi	9fb7c97669cc3cd6f55eed926e8cb947
Nessus-6.3.6-x64.msi	d03486cc224400b312513e86e0afe257
NessusAgent-6.3.6-Win32.msi	c6e5b92c97ab27768cf617a8cca34e8a
NessusAgent-6.3.6-x64.msi	e64219aa045c1aa43fcba5b0b8dab9f6

Nessus 5.2.11 Release Notes - 5/26/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Upgrade SQLite to 3.8.10.1+ - This addresses two vulnerabilities found in SQLite; see https://osvdb.org/122106 and https://osvdb.org/122105. See the Security Advisory for more information.

File Names & MD5 Checksums

File	MD5
Nessus-5.2.11-debian6_amd64.deb	d8a8aa8078e813febc516c27404e9a54
Nessus-5.2.11-debian6_i386.deb	140f5032750aeba00bfdf3fd4fefdd60
Nessus-5.2.11.dmg.gz	1076fefa3311b3a4ad40c9c3b6ede450
Nessus-5.2.11-es4.i386.rpm	d82bf31e13ea04f95813920ff8d1d76d
Nessus-5.2.11-es5.i386.rpm	e6dd371c6ac92ad049b5e551a365744e
Nessus-5.2.11-es5.x86_64.rpm	edc17fe5905c6a9fbe3f2f2d156e316b
Nessus-5.2.11-es6.i386.rpm	49c9aff99d6e606658a2eacc144d1950
Nessus-5.2.11-es6.x86_64.rpm	aca4f6b697a3a0aa8cd9fcf22c042c0c
Nessus-5.2.11-fbsd9-amd64.tbz	beac95282043923e7417938a12f4a3f3
Nessus-5.2.11-fbsd9.tbz	1ca40693256f7adf71bafc21343b6ef4
Nessus-5.2.11-fc16.i386.rpm	5c1052b485d5fe39bbbf0d8032b42f95
Nessus-5.2.11-fc16.x86_64.rpm	0892233691fccf5bb84a49ad43e5f9e7
Nessus-5.2.11-suse10.x86_64.rpm	dda769e6c28a2260f648b3820205428a
Nessus-5.2.11-suse11.i586.rpm	ab683f554b3657a19d4cdf2afc4b4549
Nessus-5.2.11-suse11.x86_64.rpm	98a484774c0fb7845f7d4348cfbc4720
Nessus-5.2.11-ubuntu1110_amd64.deb	7145798533de3f4855f66bf44ccfd5b6

File	MD5
Nessus-5.2.11-ubuntu1110_i386.deb	c7bf631563b0ce48f9d9ffbf96f6861c
Nessus-5.2.11-ubuntu910_amd64.deb	6528a8034956b1666c96af39464f1683
Nessus-5.2.11-ubuntu910_i386.deb	16b3470fe334ea38f99f7dd975ab1bcf
Nessus-5.2.11-Win32.msi	09478d3e03251ca519ac9e8639d82947
Nessus-5.2.11-x64.msi	e43b55aeacc191ac0401f7c5c284887c

Nessus 6.3.7 Release Notes - 5/26/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features, Improvements, Platform Support

- Add support for OVAL files to SCAP templates - Users can upload OVAL files to SCAP policies for Windows and Linux.

Bug Fixes

- Upgrade SQLite to 3.8.10.1+ - This addresses two vulnerabilities found in SQLite; see https://osvdb.org/122106 and https://osvdb.org/122105. See the Security Advisory for more information.
- Managed scanners may fail to sleep when not busy - Affects Nessus scanners running version 6.3.0 to 6.3.6 managed by a Nessus instance running a version before 6.3.0. This means scanners managed by Nessus Manager or Nessus Cloud won't be affected.

File Names & MD5 Checksums

File	MD5
Nessus-6.3.7-debian6_amd64.deb	97b76f932fdfc4a4dcef331558f20a3c
Nessus-6.3.7-debian6_i386.deb	ae4b08dc4b3d4b3fdcf38d5db55649d1
Nessus-6.3.7.dmg.gz	8476c1f679182da91f43b5a86bbcdfce
Nessus-6.3.7-es5.i386.rpm	0c32f2e340543a4179f8d51c7c9359fe

File	MD5
Nessus-6.3.7-es5.x86_64.rpm	b3796782f64794468328a6a6f3f3a962
Nessus-6.3.7-es6.i386.rpm	c401a8e6e5207b33af47533666561541
Nessus-6.3.7-es6.x86_64.rpm	d143de044e88bab0c9849521e857eb06
Nessus-6.3.7-es7.x86_64.rpm	b4e36faeca75fa22a89dc7131b420f14
Nessus-6.3.7-fbsd10-amd64.txz	3a5b17205834730a021b1f53904fe557
Nessus-6.3.7-fc20.x86_64.rpm	583c26ba562c15372e3496a02baa216d
Nessus-6.3.7-suse10.x86_64.rpm	578f6fc20bad2b343ef67a4171202f91
Nessus-6.3.7-suse11.i586.rpm	026be7fe063324d88040dc962e5d8f50
Nessus-6.3.7-suse11.x86_64.rpm	1b4c784f7d800181191c2363c9c9c7e6
Nessus-6.3.7-ubuntu1110_amd64.deb	d532020e1d6b067a14054e32a2a768f8
Nessus-6.3.7-ubuntu1110_i386.deb	20950df4bd447903050cc12aa6686036
Nessus-6.3.7-ubuntu910_amd64.deb	dad188776ead3c4175088643a100d684
Nessus-6.3.7-ubuntu910_i386.deb	fe6dea8e5bdbc2fb2ea47ed849c85ab4
Nessus-6.3.7-Win32.msi	e89ab91cab3d78adf69189b43cd80899
Nessus-6.3.7-x64.msi	b3a334282393b18aa27e6fdd202e491b
NessusAgent-6.3.7-Win32.msi	1e21c36565b7a021377d2c7962cd171e
NessusAgent-6.3.7-x64.msi	cf395634f3f536c4dcd94405d6598896

Nessus 6.4.0 Release Notes - 6/30/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features, Improvements, Platform Support

- AirWatch MDM Audits
- MobileIron MDM audit

- Cloud Services Audit - RackSpace Configuration Assessment
- Auditing open ports on Linux/Unix
- Add ability to copy scans
- Support CyberArk as an External Credential Store in Nessus
- Import Nmap results into Nessus to seed scan knowledge base
- Agents for OS X
- Agents for RHEL
- Agents for Fedora
- Allow users to copy Nessus Scans
- Allow access to Nessus APIs via API tokens
- Allow filtering scan results by CWE
- Registration page should include how to get activation code
- Credentialed Patch Audit Template should add assessment page to handle false positives
- Update plugin output host links
- Allow users to toggle line and bar displays for historical charts
- Include Nessus build number in version information in UI, properties api
- Document switches that can be provided to agent installer command line
- Add support for TLS 1.2 to Nessus
- Improve efficiency of scan report upload to manager

Bug Fixes

- Improved compatibility with SecurityCenter for exported policies
- Improved Scan Dashboard queries
- Improved Nessus Agent scalability and results display
- Improved Nessusd stability
- Improved SSH credential handling

- Improved differential scan selection
- Imported scans do not display the correct start and end times
- Update 'Credentialed Patch Audit' to use only the credentials provided in the policy
- Scan fragile devices is enabled by default in templates that aren't using a the 'custom' discovery view.
- Disabling a scan job from the 'Scan' view by selecting the job, clicking more->disable, does not disable the job.
- Charts are blurry on high-density displays
- Plugin archives uploaded through the UI fail to install
- For an expired activation with auto_updates disabled a new activation key will not show in UI as updated.
- Remote Scanners now honor proxy settings
- Compliance plugins no longer shown as vulnerabilities

File Names & MD5 Checksums

File	MD5
Nessus-6.4.0-debian6_amd64.deb	f3c8590d386ac4b7bb34d5f559a71fe0
Nessus-6.4.0-debian6_i386.deb	dcb6eed64bdf48409a86c218fb994e79
Nessus-6.4.0.dmg.gz	ebd5adf810f4b72b253a38d617b7952b
Nessus-6.4.0-es5.i386.rpm	cbb28925bea3fd43dd92437bd625af15
Nessus-6.4.0-es5.x86_64.rpm	bbba8e51a312d52d5ab25ab802c21abd
Nessus-6.4.0-es6.i386.rpm	f6d6072c9bcc6c808212291eb76ee95f
Nessus-6.4.0-es6.x86_64.rpm	1b3e38cb0d7c67e5f244f48fb3fe2faa
Nessus-6.4.0-es7.x86_64.rpm	5766042595c1341c1d0372679b1fdbee
Nessus-6.4.0-fbsd10-amd64.txz	0c5175e79c0274e345f7b22c9d4d6643
Nessus-6.4.0-fc20.x86_64.rpm	05287d5e21ae0e13dd6397a44fe12a0c

File	MD5
Nessus-6.4.0-suse10.x86_64.rpm	e35bb56dd2ad10d28ba88525ad11eb23
Nessus-6.4.0-suse11.i586.rpm	9fa6bf8df533372685a3d6539be31cc5
Nessus-6.4.0-suse11.x86_64.rpm	b8299e167a6cb7357bbe2de69427bff0
Nessus-6.4.0-ubuntu1110_amd64.deb	bf2d4d38d2ed02aab15e6b4bb103fd94
Nessus-6.4.0-ubuntu1110_i386.deb	1ab01d9d102fe34fc854c0ffc6233e01
Nessus-6.4.0-ubuntu910_amd64.deb	7ca665d7bfdaf023a803c072f10f5ed8
Nessus-6.4.0-ubuntu910_i386.deb	0cdd143d093b376a1c42f44f09c1be01
Nessus-6.4.0-Win32.msi	707abda1b201e9a6693413145e3d3ae7
Nessus-6.4.0-x64.msi	53c4ec3d8c74c65532bd6f834ff0adf5
NessusAgent-6.4.0.dmg.gz	8b121b8f4b852d2521a71f6f38261e53
NessusAgent-6.4.0-es5.i386.rpm	3a1151bd5460693e609fb27d3d1e10b1
NessusAgent-6.4.0-es5.x86_64.rpm	a9f18fad653d95980f2b35e6c338d373
NessusAgent-6.4.0-es6.i386.rpm	66e48efa032fda9aefc832db3112ceed
NessusAgent-6.4.0-es6.x86_64.rpm	7624b4ae30682e248087f40c8306f131
NessusAgent-6.4.0-es7.x86_64.rpm	b04a47d754fdba872ee84c21ed8acae3
NessusAgent-6.4.0-fc20.x86_64.rpm	c9abaecc4570077d95367c8a0860eed7
NessusAgent-6.4.0-Win32.msi	dfa3c55a8f26ac97d2a582ea8e5bef1b
NessusAgent-6.4.0-x64.msi	5faf19d88be1ea9ac16bb94114565e0e

Nessus 6.4.1 Release Notes - 7/2/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Fixed issue where agent may not restart after plugin update.

File Names & MD5 Checksums

File	MD5
Nessus-6.4.1-debian6_amd64.deb	2eb0413666e287751ee2d623d260ea73
Nessus-6.4.1-debian6_i386.deb	29ac5556c9c3a43036cee8e868aceae7
Nessus-6.4.1.dmg.gz	93b9f0812dcf36727935c80c37483561
Nessus-6.4.1-es5.i386.rpm	7e1d04d16f7ebc11460b41df749a6916
Nessus-6.4.1-es5.x86_64.rpm	922c47f369550743ac505b90d06060ca
Nessus-6.4.1-es6.i386.rpm	83a8aeee4d35f69353fff7c9c5388098
Nessus-6.4.1-es6.x86_64.rpm	f409dbe5099e89935dd1bd4385a0e429
Nessus-6.4.1-es7.x86_64.rpm	0bb0fe8abcd7a390a486d638976c1627
Nessus-6.4.1-fbsd10-amd64.txz	ee6287d712dfc804fb1a03bfb242f65b
Nessus-6.4.1-fc20.x86_64.rpm	61bc645b4936045fc31026aa410e5e2e
Nessus-6.4.1-suse10.x86_64.rpm	4eee7521bd84ba4875b10f5655e9803e
Nessus-6.4.1-suse11.i586.rpm	6247440711fc529f6868be1e3199166b
Nessus-6.4.1-suse11.x86_64.rpm	3f274bbd6b7c22384381a94ce289a2b6
Nessus-6.4.1-ubuntu1110_amd64.deb	59b6820c4f7ae96217a1a6f16dbe024b
Nessus-6.4.1-ubuntu1110_i386.deb	257bedf936340f2adbfb95d586f5edf3
Nessus-6.4.1-ubuntu910_amd64.deb	749efae23cec13745a976a38075257be
Nessus-6.4.1-ubuntu910_i386.deb	55e7fe7d2698569e0780380b071de6f0
Nessus-6.4.1-Win32.msi	4ef4296157e2901ce25b51d282391a09
Nessus-6.4.1-x64.msi	45df56ddecae7fcfc0ac2550f0dd7522
NessusAgent-6.4.1.dmg.gz	4c9bab2ea1987bc5370ac31e9b797536
NessusAgent-6.4.1-es5.i386.rpm	d38f4b553043da38e0075c318ba5935d
NessusAgent-6.4.1-es5.x86_64.rpm	315add60ab7c6273deb1f57ff57c7a81

File	MD5
NessusAgent-6.4.1-es6.i386.rpm	21b4ffe93110041877a20920f7fd5ee6
NessusAgent-6.4.1-es6.x86_64.rpm	f342fc937d921722881a5f3600e7f1d4
NessusAgent-6.4.1-es7.x86_64.rpm	bf8a7c0eab7739e8b8ebefc642d95ef4
NessusAgent-6.4.1-fc20.x86_64.rpm	17b36299fe690fb096142a10f75b8460
NessusAgent-6.4.1-Win32.msi	3af46a0482e775125a45f37ed98a68ec
NessusAgent-6.4.1-x64.msi	3837dffc15b724678fdb6218c52fd0e7

Nessus 5.2.12 Release Notes - 7/7/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Updates OpenSSL to remediate issues outlined in OpenSSL security advisory "secadv_20150611". See the Tenable Security Advisory for more information.

File Names & MD5 Checksums

File	MD5
Nessus-5.2.12-debian6_amd64.deb	cb2df49f49830e706a48d05e79d86481
Nessus-5.2.12-debian6_i386.deb	bdeb0d272c1d3366c83072768f9cfbda
Nessus-5.2.12.dmg.gz	4268868da2f5e043514735258649d27c
Nessus-5.2.12-es4.i386.rpm	796920741436d4ee0b682d17b49aa964
Nessus-5.2.12-es5.i386.rpm	d8da8e14701fe7c34ad0c9fdc0641111
Nessus-5.2.12-es5.x86_64.rpm	9ed71bbea92d8a2b49b8cd3ec136fa29
Nessus-5.2.12-es6.i386.rpm	49793f70039e142a26897fd381494359
Nessus-5.2.12-es6.x86_64.rpm	ecbf5ea686778a03eaae2b9d81645605
Nessus-5.2.12-fbsd9-amd64.tbz	63f1559e54e2f0016062e9ea5c565ab5

File	MD5
Nessus-5.2.12-fbsd9.tbz	0e81c938a9e429fe0cc9604014db64df
Nessus-5.2.12-fc16.i386.rpm	933ccc565093c6a9fe43621e01e4ff5b
Nessus-5.2.12-fc16.x86_64.rpm	62bd0e30f9bacf2f2bc058b9127bf2eb
Nessus-5.2.12-suse10.x86_64.rpm	d4a88fbebccc870793bba22ba55bc2bb
Nessus-5.2.12-suse11.i586.rpm	a497323d52fb993180d684920eee70d6
Nessus-5.2.12-suse11.x86_64.rpm	591f07e46a4b7bed8f221dc6034516f4
Nessus-5.2.12-ubuntu1110_amd64.deb	b465132ed6b3d3661f36a995f70f47b6
Nessus-5.2.12-ubuntu1110_i386.deb	0f0e8eb24c789ba39254b8d16566e6da
Nessus-5.2.12-ubuntu910_amd64.deb	918438d34d07012c4af7f9389945c98d
Nessus-5.2.12-ubuntu910_i386.deb	d548919ec883f43fc1bb49149e27e0d3
Nessus-5.2.12-Win32.msi	2c6c43da094aeb9fe399554692910e67
Nessus-5.2.12-Win32_XP2K3.msi	239449e3319796dbc85f667d82724b21
Nessus-5.2.12-x64.msi	dac1013c9e2e64de9083451bb8cecec1
Nessus-5.2.12-x64_XP2K3.msi	0a9113f604d616faeb9ae965b15b1480

Nessus 6.4.2 Release Notes - 7/15/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Update OpenSSL to 1.0.1p
- Improved resource management during server reloads
- Improved host discovery scan performance
- Fix issue with importing large .nessus files

File Names & MD5 Checksums

File	MD5
Nessus-6.4.2-debian6_amd64.deb	fcae7f76bf7696c6ba5ea052a58dcb73
Nessus-6.4.2-debian6_i386.deb	8b53e370f31d390def48b33da1d88eb6
Nessus-6.4.2.dmg.gz	6e40f60317c346d4b0e6b85bcadf757a
Nessus-6.4.2-es5.i386.rpm	7a4eab2d1299f64ec6616d9468f1bc59
Nessus-6.4.2-es5.x86_64.rpm	3963aa0a469fba07c0039df8464ff128
Nessus-6.4.2-es6.i386.rpm	cf65ff23a37eb9bb3ad207615f33a777
Nessus-6.4.2-es6.x86_64.rpm	9afbc8993531e965787a484833400f48
Nessus-6.4.2-es7.x86_64.rpm	c1dff4261ca6882ab5c765c0a998122e
Nessus-6.4.2-fbsd10-amd64.txz	775018165f76fffadb4e4f04f47da7e1
Nessus-6.4.2-fc20.x86_64.rpm	e624eb041a900db7178b7ae7e6f5d9f9
Nessus-6.4.2-suse10.x86_64.rpm	aacd6ed3995f226497d74dc352928655
Nessus-6.4.2-suse11.i586.rpm	0019bc6c3bdf2fd3fcf4f4f9c2d372c7
Nessus-6.4.2-suse11.x86_64.rpm	766d516d12c29467df15d78167afac4c
Nessus-6.4.2-ubuntu1110_amd64.deb	80c55930dfe210f522e0944ff82c3f25
Nessus-6.4.2-ubuntu1110_i386.deb	f51f2df3b2ab67eb7e61d3c694d81d5e
Nessus-6.4.2-ubuntu910_amd64.deb	5fc86eada4cee99eaf93cdf6dfce6a4b
Nessus-6.4.2-ubuntu910_i386.deb	cb37067d5787bf3a12648d9ddfc5bad4
Nessus-6.4.2-Win32.msi	1559ab98a6e006231574652a4cc1e06b
Nessus-6.4.2-x64.msi	558d55da8c5d42eeb484083aaf393ee8
NessusAgent-6.4.2.dmg.gz	3f60dabc08cc7542f81cf29aee608dd2
NessusAgent-6.4.2-es5.i386.rpm	0b28feb90740c4630c0971e3e0c5e0ac
NessusAgent-6.4.2-es5.x86_64.rpm	823855ea87083d62f515dbccd75fd6ee

File	MD5
NessusAgent-6.4.2-es6.i386.rpm	27a5712ac1e63b703de9ffd16490ab8c
NessusAgent-6.4.2-es6.x86_64.rpm	643151eea0619a679661533d7bc760df
NessusAgent-6.4.2-es7.x86_64.rpm	cf1ea4e260daac94db83e741d096f29e
NessusAgent-6.4.2-fc20.x86_64.rpm	1bc71762656aa974a5ba74c470a6eeed
NessusAgent-6.4.2-Win32.msi	e027adb47cafe1803b0a07c46a4f6fff
NessusAgent-6.4.2-x64.msi	dde25f32df4469bf22a51dc9d769d5a2

Nessus 6.4.3 Release Notes - 8/5/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Fix issue with non-Admin permissions on Nessus Agent templates and sharing.

File Names & MD5 Checksums

File	MD5
Nessus-6.4.3-debian6_amd64.deb	30bc538e1090a2b1222e5bb8e286f752
Nessus-6.4.3-debian6_i386.deb	121c17f48606c9d0ec9525cb458b0265
Nessus-6.4.3.dmg.gz	ebfc259fa9c615b2ea371a49294303b0
Nessus-6.4.3-es5.i386.rpm	60c9e74506206814f74bd684f75ce983
Nessus-6.4.3-es5.x86_64.rpm	256230f971bc798623f643101bda4ae6
Nessus-6.4.3-es6.i386.rpm	169181c9fb052764ad875bc028cc66a9
Nessus-6.4.3-es6.x86_64.rpm	7c1552c12d6b9e7f7158470caae12564
Nessus-6.4.3-es7.x86_64.rpm	b6fc0cac871b39e7c7b7b0129aebaa6c
Nessus-6.4.3-fbsd10-amd64.txz	051b1985467de1093866669cb5128643
Nessus-6.4.3-fc20.x86_64.rpm	ef300c4ccec948ed5ee9f20e13dbc079

File	MD5
Nessus-6.4.3-suse10.x86_64.rpm	4861ed288afb97af93262f05a3f60b89
Nessus-6.4.3-suse11.i586.rpm	8c6e99756f3a59acbb0b412658bf75d6
Nessus-6.4.3-suse11.x86_64.rpm	17304db70ff79b1b2118dcac4657a9dc
Nessus-6.4.3-ubuntu1110_amd64.deb	d54e0d377189afb90850640d4329519b
Nessus-6.4.3-ubuntu1110_i386.deb	3dced2d638fe78bbe63c1b06c8c90bb5
Nessus-6.4.3-ubuntu910_amd64.deb	64d8c1476bc8787082ebb33283840cf7
Nessus-6.4.3-ubuntu910_i386.deb	a0faf2bc08c97eb173490fa016bf51cf
Nessus-6.4.3-Win32.msi	71bc7e2152d8621e5413243d1ab4cbae
Nessus-6.4.3-x64.msi	b81cfca4c785cab33dab8f164fba1288
NessusAgent-6.4.3.dmg.gz	924b784ef405d6d3206a5705c25a4c0f
NessusAgent-6.4.3-es5.i386.rpm	fc15cc622e2cdead8323ea4a3da436bd
NessusAgent-6.4.3-es5.x86_64.rpm	5d31042a43fc7ce6ffde9d0e37face34
NessusAgent-6.4.3-es6.i386.rpm	39086afd8b6ab6994e794ebe832d48a0
NessusAgent-6.4.3-es6.x86_64.rpm	81547ff68804739e50f73e119dbb150b
NessusAgent-6.4.3-es7.x86_64.rpm	56ce1b45c7520e32268cc84c4e53a7de
NessusAgent-6.4.3-fc20.x86_64.rpm	3e3e0bb15e90f58eca08f52fad11b35b
NessusAgent-6.4.3-Win32.msi	0253313c35000527ac684502020c1c76
NessusAgent-6.4.3-x64.msi	98a015202f1bd3b32442c47e9313cc7d

Nessus 6.5.0 Release Notes - 10/12/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features, Improvements, Platform Support

- Agents for Ubuntu, Amazon Linux, and Debian
- Two-factor Support in Nessus Cloud via SMS and email
- Application Black and White Listing for Airwatch and MobileIron MDM
- SSO for Nessus Cloud via SAML
- Allow Nessus Cloud users to reset password from Nessus Cloud
- Cloud Services Audit - Microsoft Azure Configuration Assessments
- Apple Profile Manager MDM audit
- Allow managed scanners to be linked with Nessus Cloud/Manager via command line
- Excluded aborted/failed scans from trends
- Add Trend Indicators to Scan Dashboards
- Add "type" parameter to GET /scans to distinguish between agent and active scans
- Log job name and UUID when writing scan progress logs in nessusd.messages
- Display scan stop/start times with timezone setting of manager instead of remote scanner.
- Brute Force: Only use credentials provided by the user added to Credentialed Patch Audit template
- Notify user of failure if Windows Agent fails to link during install
- Add auto update frequency option to "Software Update" in settings
- On-demand scans default to not launching after being created

Bug Fixes

- In Nessus 6.4.2 and 6.4.3, Agent scans opened before scan completion could hang in Remediation query
- Plugin archives with sizes aligned to a specific byte boundary would fail to decompress
- Corrections to UI text
- Reduced CPU utilization for some platform configurations
- Updated API documentation

- Fixed error when linking to Nessus Cloud via a proxy
- Unable to delete a large number of Historical Scan data results in certain circumstances
- Nessus was generating an incorrect date for email.
- Fixed problem with policy import in SecurityCenter scans taking a long time, showing up in SecurityCenter as "Resolving hostnames"
- Nessus status not displayed correctly in preference pane on OS X when upgraded from a version prior to 6.4
- Specifying a username of "admin" in Palo Alto credentials interfered with SSH keys

File Names & MD5 Checksums

File	MD5
Nessus-6.5.0-debian6_amd64.deb	840d631d8158a07eb1a8a9c375476c29
Nessus-6.5.0-debian6_i386.deb	a4b8458fcb52ba878dcb14a8d495d15a
Nessus-6.5.0.dmg.gz	34392ffbe5422b63fc302747e5eaf871
Nessus-6.5.0-es5.i386.rpm	a32fa312f787dffe998c7d4ed5bc5f85
Nessus-6.5.0-es5.x86_64.rpm	d48ee2afaec649e1b90734cb1d44403d
Nessus-6.5.0-es6.i386.rpm	13207e7281a3c83c1345db9b863e6da3
Nessus-6.5.0-es6.x86_64.rpm	5b3e0b7ce2783237b40fc7edb42484b9
Nessus-6.5.0-es7.x86_64.rpm	79a838b0bc7c0ab85a6c6d254b80e0aa
Nessus-6.5.0-fbsd10-amd64.txz	493e143756e11f76d53e43e465aefabe
Nessus-6.5.0-fc20.x86_64.rpm	e5fc29e7348a08b6ef2cb39044e5a65e
Nessus-6.5.0-suse10.x86_64.rpm	9954ea25b08f879212f1292656e36cda
Nessus-6.5.0-suse11.i586.rpm	46fd78b86619f3ee8fc057481cd052df
Nessus-6.5.0-suse11.x86_64.rpm	62349f7f04cdac95f380da88c4a4ed45
Nessus-6.5.0-ubuntu1110_amd64.deb	a7430e3f1a7ed2123960d84d36673955

File	MD5
Nessus-6.5.0-ubuntu1110_i386.deb	aa75dbafbe3e332c022b942e943b1d84
Nessus-6.5.0-ubuntu910_amd64.deb	dcb24bc15a3bf761b03909d2cde620f2
Nessus-6.5.0-ubuntu910_i386.deb	8bfcd0a30b6c53dffa04e2965962540c
Nessus-6.5.0-Win32.msi	4bd8cc71eeb5f03e98b9a0c829d353b8
Nessus-6.5.0-x64.msi	69dce77d912b02b0ddebc1537d20cc68
NessusAgent-6.5.0-amzn.x86_64.rpm	7f54161a3568f8dd369820c69bfcaef9
NessusAgent-6.5.0-debian6_amd64.deb	ef5220ef929e86d77cc95cceabcd7472
NessusAgent-6.5.0-debian6_i386.deb	d3e007d700d79880e94325bdfd3d29fe
NessusAgent-6.5.0.dmg.gz	3f75f802667949a42db03dab7e2b9886
NessusAgent-6.5.0-es5.i386.rpm	9752979a73012d73d426b687e693adb1
NessusAgent-6.5.0-es5.x86_64.rpm	9625fb93ca562c22ccd9a04949d745fc
NessusAgent-6.5.0-es6.i386.rpm	5544dd0e557e44872188afb8ea78293c
NessusAgent-6.5.0-es6.x86_64.rpm	9134bc9f05a69b7c450e959cae523d69
NessusAgent-6.5.0-es7.x86_64.rpm	eaf3956e062cff2f714fb12e9660bbc3
NessusAgent-6.5.0-fc20.x86_64.rpm	993dae835586a976c0b13798022b70cc
NessusAgent-6.5.0-ubuntu1110_amd64.deb	68a5323253b0735a17b02ce01464bcb8
NessusAgent-6.5.0-ubuntu1110_i386.deb	50c2b34751285a2c2e3138edc0b8b4a8
NessusAgent-6.5.0-ubuntu910_amd64.deb	50c7df119b673ffd8842baad40f76927
NessusAgent-6.5.0-ubuntu910_i386.deb	7515ab8c449d645bde1f4813b9dd8587
NessusAgent-6.5.0-Win32.msi	ee7576ed33a631681712ec6706b65918
NessusAgent-6.5.0-x64.msi	8788fce525a81d347b78269afb1d5527

Nessus 6.5.1 Release Notes - 10/15/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- User with "can control" permission could cause shared scans to not execute by placing them in Trash.
- Checking Nessus daemon status on Linux broken in 6.5
- DNS lookup errors in Nessus 6.5.0 installs on Windows can prevent activation or updates
- Mobile interface not being displayed on mobile devices

File Names & MD5 Checksums

File	MD5
Nessus-6.5.1-debian6_amd64.deb	2382daca98ddd2553a51493ae1e2ac5d
Nessus-6.5.1-debian6_i386.deb	462887b4aea67eedd248997707bf602f
Nessus-6.5.1.dmg.gz	fdd48a21d45b47fff8e57389a7855f57
Nessus-6.5.1-es5.i386.rpm	cd05bbc9d75a6e90c54ba77ea5c1af80
Nessus-6.5.1-es5.x86_64.rpm	077d0b7837c2107a5b29bb411b3e28a8
Nessus-6.5.1-es6.i386.rpm	77ce003eec6ba26b78c901cfe743acdc
Nessus-6.5.1-es6.x86_64.rpm	073e6134a3fbf2be909629381b612e34
Nessus-6.5.1-es7.x86_64.rpm	9a65587d9f286f9b9e504f234f95a666
Nessus-6.5.1-fbsd10-amd64.txz	c59297c4b6f80b46a6aac4b61fe6bc36
Nessus-6.5.1-fc20.x86_64.rpm	4c76a2cf6302268f8e330cb4fed82857
Nessus-6.5.1-suse10.x86_64.rpm	4caca8fa78b8f9ca6c7c4f1eda411b58
Nessus-6.5.1-suse11.i586.rpm	19e93f234d6d39f4a7201ba61f82d990
Nessus-6.5.1-suse11.x86_64.rpm	ff9be3d00d6c89a1a83b0fff1bbd718c
Nessus-6.5.1-ubuntu1110_amd64.deb	e0cb8c41b060d131d7a6125bc1fc9461

File	MD5
Nessus-6.5.1-ubuntu1110_i386.deb	f1b448805b576ae7d20f039d61ad7d4c
Nessus-6.5.1-ubuntu910_amd64.deb	8a1e323077363422efe385d939e34f25
Nessus-6.5.1-ubuntu910_i386.deb	ae8029e8c1d65d38204c7257b6f72f37
Nessus-6.5.1-Win32.msi	42c962d4da788a72249fd00070afc0c9
Nessus-6.5.1-x64.msi	7aab4c82f9cf36f8b84abc8ff469e2f8
NessusAgent-6.5.1-amzn.x86_64.rpm	77b3e69c3a288845163076ca98b1cb70
NessusAgent-6.5.1-debian6_amd64.deb	3964a5534cbead32ec6a38bc2093205f
NessusAgent-6.5.1-debian6_i386.deb	1d14cc3bcfb63a5ec168a69fbb2d1393
NessusAgent-6.5.1.dmg.gz	d6c4f0ea78791289f4018061f760c71e
NessusAgent-6.5.1-es5.i386.rpm	a497001a36da351114ddc56e3e55ea5a
NessusAgent-6.5.1-es5.x86_64.rpm	e4d24544dd99da89f089fd9c7563e333
NessusAgent-6.5.1-es6.i386.rpm	0b145be7a9dd59a8cee2fa524753270c
NessusAgent-6.5.1-es6.x86_64.rpm	8b3f5d267b36ec7320c902f0a741d8b6
NessusAgent-6.5.1-es7.x86_64.rpm	c9067eeefd95fe730c73673431be6813
NessusAgent-6.5.1-fc20.x86_64.rpm	a7a088c0abc1d9e864e826245cc4134d
NessusAgent-6.5.1-ubuntu1110_amd64.deb	ca50f822dd49ead1b632b54bc63cfb51
NessusAgent-6.5.1-ubuntu1110_i386.deb	360969fbcba3d02f4cba99f70d3f7728
NessusAgent-6.5.1-ubuntu910_amd64.deb	0cd5d023b7996979a83d84457cb38135
NessusAgent-6.5.1-ubuntu910_i386.deb	70b38eab78bbb89d15b860583eb69168
NessusAgent-6.5.1-Win32.msi	6f5253e5f563310de293eda4186f6ecf
NessusAgent-6.5.1-x64.msi	03f0316794ec27204290f1d722d6aa99

Nessus 6.5.2 Release Notes - 10/19/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Scanners running on Windows may not scan IPv6 targets

File Names & MD5 Checksums

File	MD5
Nessus-6.5.2-debian6_amd64.deb	dad0600056fb0d902e8dab05e18c2e6a
Nessus-6.5.2-debian6_i386.deb	7bddf2260da83c48c1bbe391df490d8a
Nessus-6.5.2.dmg.gz	b738bec09e7e11dff81570ca086dd081
Nessus-6.5.2-es5.i386.rpm	725bae049b888a1d4fa15b0ecc24cc07
Nessus-6.5.2-es5.x86_64.rpm	91f8700dfd17c453f925bb5ba7a9e4fd
Nessus-6.5.2-es6.i386.rpm	4a541248d1e78de56618c5ce17489a60
Nessus-6.5.2-es6.x86_64.rpm	84e72011dd2f379e6b0f69d74b912fd7
Nessus-6.5.2-es7.x86_64.rpm	34aa86922c6d9f1e413a040e056e079b
Nessus-6.5.2-fbsd10-amd64.txz	4fd34b58c8e56478c7eed7c187ef0c14
Nessus-6.5.2-fc20.x86_64.rpm	6c3d327c4bb85e07012ea15415e6be2f
Nessus-6.5.2-suse10.x86_64.rpm	bd1376c6b165415ffff89be414122726
Nessus-6.5.2-suse11.i586.rpm	a8a5f66f39bf887292c22076de040e13
Nessus-6.5.2-suse11.x86_64.rpm	3e9d649324677a578a05fc04186a0fb5
Nessus-6.5.2-ubuntu1110_amd64.deb	9c276c3ba4a4753aab5194a90b0c92f6
Nessus-6.5.2-ubuntu1110_i386.deb	bea5d6d0236972c4d067851060e47b90
Nessus-6.5.2-ubuntu910_amd64.deb	5dd59d020116414fed7e4465e0c8a227
Nessus-6.5.2-ubuntu910_i386.deb	0a18863b74e43e57a6ba44a9cd9d4a75
Nessus-6.5.2-Win32.msi	fbf34abb6c0effd5ce681882fb906811

File	MD5
Nessus-6.5.2-x64.msi	9f6a1c03102fd1098a5c90a9f609101b
NessusAgent-6.5.2-amzn.x86_64.rpm	fec1544432a3a78662ae37adfc16e70f
NessusAgent-6.5.2-debian6_amd64.deb	9801fd2abc53042ba93291c9aefce702
NessusAgent-6.5.2-debian6_i386.deb	139a35ea724928e4224328daacafaafd
NessusAgent-6.5.2.dmg.gz	83399830fe33353d5d90d1654d938cb3
NessusAgent-6.5.2-es5.i386.rpm	b20359c1e6d153571cdb6705129fb923
NessusAgent-6.5.2-es5.x86_64.rpm	ffa4cb2464a0ba8450682f50efb9491a
NessusAgent-6.5.2-es6.i386.rpm	c0d7660a1413ed57f51b264686dc5820
NessusAgent-6.5.2-es6.x86_64.rpm	dcac964055fb9a993427027cfedba8c4
NessusAgent-6.5.2-es7.x86_64.rpm	cce854b0447a62e6c49733a3ed3ce558
NessusAgent-6.5.2-fc20.x86_64.rpm	3f6db57d738684599a743e194aaeaa4e
NessusAgent-6.5.2-ubuntu1110_amd64.deb	e4d3bd7553ac4863f405126ce4d049d2
NessusAgent-6.5.2-ubuntu1110_i386.deb	4be5fa409ab4acd3adeb75622a60cb2c
NessusAgent-6.5.2-ubuntu910_amd64.deb	8f7c2be815c9bc947287dfa070c8cc8a
NessusAgent-6.5.2-ubuntu910_i386.deb	8a72da31c8e63f0d562d65d89c8fd696
NessusAgent-6.5.2-Win32.msi	1bf4bfeb5b852e3d0e763dc204f984c8
NessusAgent-6.5.2-x64.msi	1554e05c799febcf7b5e797ea054eb63

Nessus 6.5.3 Release Notes - 11/10/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- SecurityCenter attempts to manage Nessus Manager instances connected for agent scans imports
- DNS resolution may fail on OS X due to inadequate timeouts

- Attempts to allocate large blocks of memory can cause the nessusd daemon to terminate
- Unable to enable SSL for IBM Tivoli connections

File Names & MD5 Checksums

File	MD5
Nessus-6.5.3-debian6_amd64.deb	5c3fadcc460c0c61b2209dc7a9ac622f
Nessus-6.5.3-debian6_i386.deb	d28aa9083ab6dd85bfef23a7ff45b459
Nessus-6.5.3.dmg.gz	fb1780c9a74f132292371db961066f3c
Nessus-6.5.3-es5.i386.rpm	c2375f45446ecdb78d2587dd679d2562
Nessus-6.5.3-es5.x86_64.rpm	5e2d6d6cb4a9761c1c7712a961e603d7
Nessus-6.5.3-es6.i386.rpm	afd58f5d9f8985cf3d49250eee8bed72
Nessus-6.5.3-es6.x86_64.rpm	722d72d63cb1bc235f4d76fd1a8ea6ae
Nessus-6.5.3-es7.x86_64.rpm	65e83c56fe529aae6cd2324137614665
Nessus-6.5.3-fbsd10-amd64.txz	ece54256bf521f2163ef8f8a144baae0
Nessus-6.5.3-fc20.x86_64.rpm	9dc5d9f0838fed8432a22e2748aad303
Nessus-6.5.3-suse10.x86_64.rpm	c7db4bfb6e60c3e5a7ca54dbc1ab3bdc
Nessus-6.5.3-suse11.i586.rpm	e4ef1f0231959a01e8e0898fd261c008
Nessus-6.5.3-suse11.x86_64.rpm	132370a13595866b81c74d0826984caa
Nessus-6.5.3-ubuntu1110_amd64.deb	fa3e93a6725fafdef33dd68388970c90
Nessus-6.5.3-ubuntu1110_i386.deb	beab0830f343ef33f0fc57dc01883443
Nessus-6.5.3-ubuntu910_amd64.deb	3c079f2716c45de680bad2bfa9ff7dbb
Nessus-6.5.3-ubuntu910_i386.deb	357f2c8d8df5a08379a4effc52e581d3
Nessus-6.5.3-Win32.msi	17957bf4f1ec076ce3447764dde913f4
Nessus-6.5.3-x64.msi	5cc06b44d4c68ba103b24cf104aab8a7
NessusAgent-6.5.3-amzn.x86_64.rpm	516de1956aafa46016bd251b6f94c139

File	MD5
NessusAgent-6.5.3-debian6_amd64.deb	d8a7eb652a2dff62bcbae50a8271a968
NessusAgent-6.5.3-debian6_i386.deb	4defaf548e112db921b28b7254ead872
NessusAgent-6.5.3.dmg.gz	3bd3f3d1e43f7beda169122d5fcc30e6
NessusAgent-6.5.3-es5.i386.rpm	09f9ebc3c3a6ba84f7da8cc8d44b0cf4
NessusAgent-6.5.3-es5.x86_64.rpm	33ad787b46ab25744449ed856fccc065
NessusAgent-6.5.3-es6.i386.rpm	f62c321c5f3988df27c3da5e5f99c5c9
NessusAgent-6.5.3-es6.x86_64.rpm	0b7179088f3d246c6b8e73410dc200e7
NessusAgent-6.5.3-es7.x86_64.rpm	fd227bbced2f5d63bf308432cda44507
NessusAgent-6.5.3-fc20.x86_64.rpm	2942377a3b475f0b90c68714d726cf52
NessusAgent-6.5.3-ubuntu1110_amd64.deb	210dbb7b2cca647ea8343f794ecad756
NessusAgent-6.5.3-ubuntu1110_i386.deb	c7f1fa82d23d3733ca8554b0b5b63ae0
NessusAgent-6.5.3-ubuntu910_amd64.deb	14135eaabaf3312ba433a2aba0a2475e
NessusAgent-6.5.3-ubuntu910_i386.deb	7e5ad6134c10e03bc1e782230b084a2b
NessusAgent-6.5.3-Win32.msi	c865d811fa163735a3196e6183b9d3e2
NessusAgent-6.5.3-x64.msi	29675b7826266849c4b260a38c50fe37

Nessus 6.5.4 Release Notes - 12/14/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features/Expanded Platform Support

- Add support for Nessus and Nessus Agents on El Capitan

Bug Fixes and Improvements

- Address issues with IPv6 scanning on Windows and FreeBSD 102
- Fixed issue with adding Kerberos authentication introduced in Nessus 6.5.3

- Correctly handle scan results for usernames containing "+" characters
- Fixed issue with display of agent results for some groups

File Names & MD5 Checksums

File	MD5
Nessus-6.5.4-debian6_amd64.deb	544e91f5a2ce91cdfce6ba1a780411e0
Nessus-6.5.4-debian6_i386.deb	b356bfebccd2c92b6b9566dd361323cd
Nessus-6.5.4.dmg	aca32b8e6b525a622c7719f2790b3e5e
Nessus-6.5.4-es5.i386.rpm	c2b3c90207a9fdc13e4d27daa78080fd
Nessus-6.5.4-es5.x86_64.rpm	c48002d761daa791198c2c2de4ad73db
Nessus-6.5.4-es6.i386.rpm	8294300ae5981c8eeacf72a53337b3ec
Nessus-6.5.4-es6.x86_64.rpm	c99527ae789e120e03bfa5a73bef2c84
Nessus-6.5.4-es7.x86_64.rpm	2fb6ae5817d6a1ab3cc67464e87a7297
Nessus-6.5.4-fbsd10-amd64.txz	3868f5a2270e24ccee65475e70d01327
Nessus-6.5.4-fc20.x86_64.rpm	959333b121765ad25d0a0ff8973cfb56
Nessus-6.5.4-suse10.x86_64.rpm	d69ab2ee96d842eb51029d7544affee2
Nessus-6.5.4-suse11.i586.rpm	612502e8ae4210e0330b3b1d1b32ab85
Nessus-6.5.4-suse11.x86_64.rpm	ea1561e71f7bbf654a93a944d728bacc
Nessus-6.5.4-ubuntu1110_amd64.deb	20933d20300745f4cc5a38007c4abe8d
Nessus-6.5.4-ubuntu1110_i386.deb	6a95e2dacfa07e4ab613395b72180899
Nessus-6.5.4-ubuntu910_amd64.deb	0e5142c1b1c82dd1d54fb17dad106a6c
Nessus-6.5.4-ubuntu910_i386.deb	9b76207ec0c2ab0257814b6335fa165b
Nessus-6.5.4-Win32.msi	06b4c5ee2816541779ab10df2ff76e15
Nessus-6.5.4-x64.msi	146e83f33db62fbb692460f2d5a4539c
NessusAgent-6.5.4-amzn.x86_64.rpm	a301078367b1cbb3f7fc3e0d076e9783

File	MD5
NessusAgent-6.5.4-debian6_amd64.deb	92c4e9856f4db1b8252928efdc6c0240
NessusAgent-6.5.4-debian6_i386.deb	7c66a1a41ce70530ec22dfa7d747edbb
NessusAgent-6.5.4.dmg	ba8aa8d557ba6a4b4acc670a6051ae39
NessusAgent-6.5.4-es5.i386.rpm	761ef94aba77f05b5c5d83cf5ca223c6
NessusAgent-6.5.4-es5.x86_64.rpm	0b7d41c6cfd5ef764e2696c6a9a76308
NessusAgent-6.5.4-es6.i386.rpm	471498db0f41a6908fc6b15f4619cd08
NessusAgent-6.5.4-es6.x86_64.rpm	51942c4630168ebd0abf14c14988c311
NessusAgent-6.5.4-es7.x86_64.rpm	897bc1e93a312305607ee034ec0640d5
NessusAgent-6.5.4-fc20.x86_64.rpm	fdc6e6f5db07c8471710c6c9187d64c3
NessusAgent-6.5.4-ubuntu1110_amd64.deb	268a7828c741a729e0a84117c342d8dd
NessusAgent-6.5.4-ubuntu1110_i386.deb	2f204f45add0dd84a7d8735ecf256812
NessusAgent-6.5.4-ubuntu910_amd64.deb	aebf542cf3c4e4fc02378b7b59609913
NessusAgent-6.5.4-ubuntu910_i386.deb	2ad27879bc437e3956ed013282b9b438
NessusAgent-6.5.4-Win32.msi	6a04fcd56f298828f2fcbe9ce3bb5091
NessusAgent-6.5.4-x64.msi	587535cd2f1912461b0bf387c0508dd4

2014 Tenable Nessus

Nessus 6.0.2 Release Notes - 11/10/2014

Nessus 6.1.0 Release Notes - 11/18/2014

Nessus 6.1.1 Release Notes - 12/2/2014

Nessus 6.1.2 Release Notes - 12/15/2014

Nessus 5.2.5 Release Notes - 1/20/2014

Nessus 5.2.6 Release Notes - 3/24/2014

Nessus 5.2.7 Release Notes - 6/12/2014

[Nessus 6.0.0 Release Notes - 10/14/2014](#)

[Nessus 6.0.1 Release Notes - 10/20/2014](#)

Nessus 6.0.2 Release Notes - 11/10/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This release fixes the following issues:

- Registration does not go through Proxy server
- Slow Nessus 6 UI
- Designate hosts by their DNS name is sometimes not working, in cases where it did in 5.2.x

Nessus 6.1.0 Release Notes - 11/18/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- Cisco ISE Integration
- Updated Settings View
- Enhanced Launch control in Scan Details
- Update scan export

Improvements

- Updated plugin output behaviour

Bug Fixes

- Nessus Enterprise not allowing LDAP login of added users
- Remote scanner fails to upload reports bigger than 2.1G
- DELETE /scan/{scan_id}/history/{history_id} is missing from API Browser
- Risk Factor is not included in the drop-down list for email notifications
- Nessus 6 email notifications contain broken links

- Nessus 5.0 API /plugins/description call is missing in 6.0 API
- Add File for Upload Targets is absent in IE9
- Invalid xml export from Nessus 6
- Scheduled scans run from trash

File Names & MD5 Checksums

File	MD5
Nessus-6.1.0.dmg.gz	420966f32dd4637d1ab52154df1ebd06
Nessus-6.1.0-debian6_amd64.deb	5e0c1f95d0ba9c64fdae7233a060769a
Nessus-6.1.0-es5.x86_64.rpm	b994f9e2bd279dcb6291f21e3bab98d0
Nessus-6.1.0-es6.x86_64.rpm	c2c543317f147252e6b99f119c7bf944
Nessus-6.1.0-es7.x86_64.rpm	2192f7978bc7c94925c189228adf7ea9
Nessus-6.1.0-fbsd10-amd64.txz	73ce698860373009c98e35354a59b1e3
Nessus-6.1.0-fc20.x86_64.rpm	7f583481855d90c31d153e9fee0264d8
Nessus-6.1.0-suse10.x86_64.rpm	4f2fea36fc45dba25aff91b0c998839e
Nessus-6.1.0-suse11.x86_64.rpm	5961a85bc61bee27dbef6dc942a1b442
Nessus-6.1.0-ubuntu1110_amd64.deb	af3d407b62c713f547e14c8a1a9b37d1
Nessus-6.1.0-ubuntu910_amd64.deb	2bfa439a6e7f37660718a933b392e6e0
Nessus-6.1.0-x64.msi	7c6162caedf613db3b9dab21c89bbb00

Nessus 6.1.1 Release Notes - 12/2/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Show msagent scans in scanner scan list
- Nessus Scanner managed by SecurityCenter: Settings-Overview shows N/A

- Cisco ISE requests are still made if no ip address for the host
- GET /policies/{id} plugins response is incorrect
- API /scans/import returns id that does not match the id from /scans
- Edit Password does not check confirm field
- Users can not edit a vulnerability in host view
- Internal PCI Policy Template Credentials Not Working
- Remote scanner upload race condition

File Names & MD5 Checksums

File	MD5
Nessus-6.1.1-debian6_amd64.deb	bef642d486e6cc2044b6bd3ee7e1ece2
Nessus-6.1.1-es5.x86_64.rpm	b3ad3f9352dc709892187e1281229662
Nessus-6.1.1-es6.x86_64.rpm	4565b86cb86f07bd2caebe0257b68e11
Nessus-6.1.1-es7.x86_64.rpm	3eae135e9ecfe46b5afe1d2f0ffaace8
Nessus-6.1.1-fbsd10-amd64.txz	52abb4f9e0ebe1797fa1dbb746316cf2
Nessus-6.1.1-fc20.x86_64.rpm	986bf61503c7465b49d2af311c670e0b
Nessus-6.1.1-suse10.x86_64.rpm	35b7a7f4b6f1745c3763bb1941ab3d85
Nessus-6.1.1-suse11.x86_64.rpm	05c7600dc1adf91f1f5591ac93a10b01
Nessus-6.1.1-ubuntu1110_amd64.deb	c153f3f38b8d359792bde8b3faec30f7
Nessus-6.1.1-ubuntu910_amd64.deb	5349b2e81e0dbe80234de74dbdbb0f0d
Nessus-6.1.1-x64.msi	62b28c7a0b24cfd643eaf9e84ab27c0d
Nessus-6.1.1.dmg.gz	c17939858586f325b4a4dadc1e812bc5

Nessus 6.1.2 Release Notes - 12/15/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Nessus 6 long scan names cause export to fail
- Remote scanner job status race condition on manager reload
- Offline config audit for fortigate is missing.
- "undefined variable skipped" message in nessusd.dump
- CVSS Temporal Vector in downloaded reports is wrong
- Issues with updates on Windows
- Remote scanners don't stop scans when job no longer exists on manager
- Cisco ISE REST calls are incorrect
- Email report generation can cause 100% CPU and hung the scanner resources
- Mixed plugin families are not saved correctly when filtering is used
- SC scans are aborted if Nessus reloads while a scan is running
- Some remote scans are aborted if being started just before a reload of the manager

File Names & MD5 Checksums

File	MD5
Nessus-6.1.2-debian6_amd64.deb	3ff0d5c7bb388f7e60081b08078dafe0
Nessus-6.1.2-es5.x86_64.rpm	95fed53b1bfcabf90fb3a3e2e1e1e15a
Nessus-6.1.2-es6.x86_64.rpm	979f77c17eb0eeb5743a3297b495b450
Nessus-6.1.2-es7.x86_64.rpm	aaf44bf482fd3ec8c01c53221f68a2ba
Nessus-6.1.2-fbsd10-amd64.txz	55b9ea89d8b9433d9619c6acb5a92827
Nessus-6.1.2-fc20.x86_64.rpm	a03ac19b78a59211325e486f8cbdca25
Nessus-6.1.2-suse10.x86_64.rpm	2034a85aafadf55a66490dae5fe5fc65
Nessus-6.1.2-suse11.x86_64.rpm	7b9b131438a40f1fa5e35b41d733b78d
Nessus-6.1.2-ubuntu1110_amd64.deb	4254d69faf853b3dace75e75b962ba88
Nessus-6.1.2-ubuntu910_amd64.deb	c9e38c3c0b47e7a0579cf308a7cb71f6

File	MD5
Nessus-6.1.2-x64.msi	a219754c6f8f8894459123f81cafbb4d
Nessus-6.1.2.dmg.gz	fa99686f39b4598674cfefdf389d5863

Nessus 5.2.5 Release Notes - 1/20/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This release fixes the following issues:

- A possible deadlock occurring under certain conditions at the end of the scan (mostly exhibited by the patches_summary.nbin plugin)
- Reduced the overall memory usage by using a different memory allocator (Linux only)
- A memory leak in webmirror has been corrected
- Fixes an issue occurring when scanning for IPv6 targets on the same local subnet (Linux)
- Fixes the cross-references in the /plugins/description API
- Switched the default plugin database to "low memory usage" (qdb_mem_usage=low) on new installations

Nessus 5.2.6 Release Notes - 3/24/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This release fixes the following issues:

- memory leak when scanning ssl enabled services
- memory leak when scanning ipv6 targets

Nessus 5.2.7 Release Notes - 6/12/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This release fixes the following issues:

- Upgrades OpenSSL to 1.0.0m to address SSL/TLS MITM vulnerability (CVE-2014-0224).
- Fixes a race condition where a scan could start but appears as aborted with no results (remote scanner under heavy use)
- Fixes a potential deadlock

Nessus 6.0.0 Release Notes - 10/14/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: The MD5.asc will no longer be available. All the packages are signed with integrity checks.

The latest version, Nessus v6, enables you to reduce your attack surface by enforcing compliance and system hardening policies. Nessus users will more easily be able to create and customize compliance and security policies while also being able to manage scan results, schedules, and policies.

Keeping Nessus v6 up-to-date is now an automated process and provides you with more control over the update process. Easily integrate Nessus into your existing security processes with a new API, which is fully documented and accessible from within the Nessus UI. A listing of the new features can be found below:

Compliance and System Hardening Policies

Hundreds of compliance and system hardening policies ("audit" files) are now available directly from the Nessus UI via the plugin feed. Nessus users can access out-of-the-box policies for network gear, firewalls, storage devices, virtualization and cloud platforms, and a wide variety of major operating system platforms (including UNIX, Linux and Windows), and much more!

Compliance and System Hardening Policy Editor

Nessus v6 simplifies the customization of policies, enabling the user to tune various compliance and system hardening policy settings from within the Nessus UI.

Automatic Updating

The Nessus engine and UI will be updated, enabling automatic or user-initiated updates.

Nessus RESTful API

Provides a standard and supported API for integrations. The XMLRPC API has been replaced with a simpler RESTful API, complete with documentation and examples available from the Nessus UI.

New Policy Editor

Simplify editing Policies. Plugin preferences and policy settings have been reorganized to improve navigation and discoverability.

Unified Scan View

Simplify creating and managing scans. Remove scan and schedule views and replace with a single view. Scans can be controlled from the scan listing. A new "History" tab shows previous results, and changes can be made via a "Configure" button in Scan Detail view.

Changelog

- Mac OS X Preferences panel: When nessus is stopped, the status text has the word vulnerabilities misspelled as vulnerabilites
- Username and Password fields are displayed when Auth Method is set to None.
- SSH Netstat portscan not reporting port 22 - Plugin 14272
- Nessus 5.2.6 can't handle SSL tunnels
- Email Filters after saving and returning, Any Changes back to All
- Error Message in UI is Spelled Incorrectly
- Description in schedule scans cannot be removed
- The NASL VM fails to receive data on SSL socket under certain conditions
- Stuck in Please wait during login.
- Nessus Enterprise users last login show NA
- Saving users in NEC is posting regardless of form errors
- After importing nessusdb or .nessus scan results, the first .nessus scan export always fails
- /scan/reset api for SC does not stop the associated scans
- Information at Settings / Scanners / Local Scanner out of sync
- HTML export takes forever when the scan result contain multiple host/vuln/outputs
- No PDF option on Nessus MAC
- Add bulk modification to scan results

Nessus 6.0.1 Release Notes - 10/20/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This release fixes the following issues:

- Nessus 6 - text field size limitation (port scan range)
- Nessus scanners managed by SecurityCenter shows up as Nessus Home in overview
- Disable SSLv3 in Web Server
- Safari 7.1 hangs during policy creation in Nessus 6

2013 Tenable Nessus

Nessus 5.2.1 Release Notes - 5/7/2013

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Nessus 5.2.1 solves the following issues:

- On Windows: it is again possible to install Nessus under a non-standard directory
- A memory leak would occur when doing a scan which creates a KB over 10 megabytes
- Fixed a stability issue in the web server

Nessus 5.2.2 Release Notes - 9/12/2013

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Version 5.2.2 provides the following improvements:

- Improved the packet capture driver on Windows 7 and newer
- Nessus now has the ability to export reports as full DBs that can be moved from one scanner to another
- New, faster web mirror plugin

This release also addresses the following bugs:

- RC4 ciphers present in the the Nessus web server
- Unable to save policy description in Flash
- Nessus sometimes enters a crash loop while trying to initialize the plugins
- Nessus registration screen does not support ampersand characters for passwords
- Some scans requested to stop get stuck in the "Stopping" state
- Parse error when importing scan results
- NASL: Long single-quoted strings have the wrong length
- NASL: query_report could lock the scan/report on error
- NASL: Using #TRUSTED causes the next line of script to be ignored
- NASL: Passing an empty string to str_replace() causes an out of bound read

Nessus 5.2.3 Release Notes - 9/30/2013

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This is a maintenance release which fixes two crash issues:

- Crash occurring on Windows Vista and newer related to packet forgery.
- In some situations, stopping a scan could lead to a deadlock or a crash.

Nessus 5.2.4 Release Notes - 10/25/2013

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This new release fixes two issues:

- A packet forgery issue occurring on Windows Vista and newer OSes. We addressed this issue by switching to the WinPcap driver
- A crash could be occurring if resolving "plugins.nessus.org" would fail

Tenable Agent Release Notes

To view EOL Tenable Agent release notes, see Tenable EOL Release Notes.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

2022 Tenable Agent

2021 Tenable Agent

2020 Tenable Agent

2019 Tenable Agent

2018 Tenable Agent

2017 Tenable Agent

Tenable Agent 10.3.2 (2023-03-09)

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.3.2:

- New links to Tenable Vulnerability Management now direct to sensor.cloud.tenable.com when you use the `--cloud` linking parameter.

Security Updates

The following are security updates included in Tenable Agent 10.3.2:

- Updated OpenSSL to version 3.0.8.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- You can upgrade to the latest version of Tenable Agent from any previously supported version.

- If your upgrade path skips versions of the Tenable Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked Tenable Agents communicate with.
  - Tenable Vulnerability Management-linked Tenable Agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. If agents versions 8.1.0 through 10.3.1 are not able to connect to the new domain, they fall back to using cloud.tenable.com. Tenable Agent 10.3.2 and later do not fall back using the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Contact your network administrator for assistance with making necessary changes to your allow list.

2022 Tenable Agent

Nessus Agent 8.3.2 Release Notes - 2022-03-03

Nessus Agent 8.3.3 Release Notes - 2022-03-31

Nessus Agent 8.3.4 Release Notes - 2022-08-25

Nessus Agent 10.1.0 Release Notes - 2022-02-02

Nessus Agent 10.1.1 Release Notes - 2022-02-10

Nessus Agent 10.1.2 Release Notes - 2022-03-03

Nessus Agent 10.1.3 Release Notes - 2022-03-31

Nessus Agent 10.1.4 Release Notes - 2022-06-15

Nessus Agent 10.2.0 Release Notes - 2022-08-02

Nessus Agent 10.2.1 Release Notes - 2022-11-02

Nessus Agent 10.3.0 Release Notes - 2022-11-17

Nessus Agent 10.3.1 Release Notes - 2022-12-12

Nessus Agent 8.3.2 Release Notes - 2022-03-03

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Nessus Agent 8.3.2:

- Updated the snappy and libxml libraries to support FedRamp certification.

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains,

reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 8.3.3 Release Notes - 2022-03-31

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Tenable Agent 8.3.3:

- OpenSSL was updated to the latest version 1.1.1n.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains,

reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 8.3.4 Release Notes - 2022-08-25

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: 8.3.4 agents linked to Tenable Vulnerability Management with an update schedule enabled will be automatically updated to version 10.1.4 or higher.

Security Updates

The following are security updates included in Tenable Agent 8.3.4:

- Addressed a vulnerability where an audit file could be used to bypass PowerShell and execute commands with elevated privileges on a local scanner.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com.

Agents with earlier versions will continue to use the cloud.tenable.com domain.

  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.

- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.1.0 Release Notes - 2022-02-02

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.1.0:

- Added NessusCLI commands for viewing installed plugin information and resetting plugin data stored on the host system.
  - https://docs.tenable.com/nessus-agent/Content/NessusCLIAgent.htm

Bug Fixes

Bug Fix	Defect ID
Resolved an issue where some Amazon Linux Agent packages were not signed correctly.	01222403
Resolved an issue where some agents would not link to a group when using the offline and group linking arguments.	01264341
Resolved an issue where some agents exhibit high CPU utilization on Openshift servers.	01287716
Resolved an issue where CA certificates included with the agent installation package did now have an updated certificate for Let's Encrypt.	01289248

Upgrade Notes

- Tenable Agents upgraded via Tenable Nessus Manager will not upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.1.1 Release Notes - 2022-02-10

Bug Fixes

Bug Fix
Fixed an issue that caused the nessus-service of Tenable Agents to fail in some macOS environments when upgrading to 10.1.0.

Upgrade Notes

- Tenable Agents upgraded via Tenable Nessus Manager will not upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.

  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.

  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.

- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.1.2 Release Notes - 2022-03-03

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Nessus Agent 10.1.2:

- Agents now only pull down plugins as they are needed for configured scans. This disk space optimization means that an agent will not automatically pull down plugins as soon as it is linked. When a scan is configured, it will pull down any plugin category or categories needed for that scan that are not already on-disk. If a plugin set is not used by an agent for 14 days, they will be automatically deleted from the agent.

Bug Fixes

Bug Fix
Fixed an issue where 10.1.1 and prior Nessus Agents without plugins would request plugin updates every minute.

Upgrade Notes

- Tenable Agents upgraded via Tenable Nessus Manager will not upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.1.3 Release Notes - 2022-03-31

Security Updates

The following are security updates included in Tenable Agent 10.1.3:

- OpenSSL was updated to the latest version 1.1.1n.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Tenable Agents upgraded via Tenable Nessus Manager will not upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.1.4 Release Notes - 2022-06-15

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.1.4:

- Enabled audit signing support for Tenable Agent to provide a secure verification capability for audit scanning files.

  For more information, see the Audit Signing Overview KB article.

Security Updates

The following are security updates included in Tenable Agent 10.1.4:

- Fixed potential agent vulnerabilities.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Tenable Agents upgraded via Tenable Nessus Manager will not upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.2.0 Release Notes - 2022-08-02

Note: As of Agent 10.2.0, Nessus Agent uses a new signing key that complies with more modern standards. To verify your Agent downloads, download the new key, `RPM-GPG-KEY-Tenable-4096`, from https://www.tenable.com/downloads/nessus-agents and import it into your command line installation toolset (for example, `rpm --import`). You can still use the legacy key, `RPM-GPG-KEY-Tenable-2048`, for Nessus Agent versions 10.1.4 and earlier.

Note: Tenable is aware of an issue where certain Linux-based agents become unresponsive after installing the EA version of Agent 10.2.0. To address this condition, reinstall the GA version of Agent 10.2.0 locally.

New Features

The following are the new features included in Tenable Agent 10.2.0:

- Added a local NessusCLI setting that allows you to disable regular metadata updates. When enabled, metadata updates only occur at linking and when the agent runs a scan. For more information, see the **Skip Asset Observation On Update** setting in the *Nessus Agent User Guide*.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.2.0:

- Added the following operating system support for agents:
  - Debian 11
  - RHEL 9
  - Ubuntu 22.04
- Added Graviton ARM support for agents on the following operating systems:
  - Red Hat/Oracle 7, 8, and 9
  - CentOS 7
  - Ubuntu 20.04 and 22.04
- Added OpenSSL 3.0.5 support.

Bug Fixes

Bug Fix	Defect ID
Resolved issue where a specific scheduler configuration would cause the agent to shut down.	5003a00001F54U1AAJ
Resolved issue where 8.x versions of agent would not install on CentOS 6.	5003a00001AeDVo

Upgrade Notes

- Nessus Agent 10.2.0 introduces a new service called `nessus-agent-module`. The new service does not impact any agent functionality or operations. If you use an allow list in a third party endpoint security product, such as AV or host-based intrusion prevention, you need to add `nessus-agent-module` to the allow list. For more information, see File and Process Allow List in the *Nessus Agent User Guide*.

- Tenable Agents upgraded via Tenable Nessus Manager cannot upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.

  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions continue to use the cloud.tenable.com domain.

  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.

- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.2.1 Release Notes - 2022-11-02

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.2.1:

- Added support for the following operating systems:
  - macOS 13

Security Updates

The following are security updates included in Tenable Agent 10.2.1:

- Updated OpenSSL to 3.0.7 to address two high-severity security vulnerabilities.

  For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Nessus Agent 10.2.0 introduces a new service called `nessus-agent-module`. The new service does not impact any agent functionality or operations. If you use an allow list in a third party endpoint security product, such as AV or host-based intrusion prevention, you need to add `nessus-agent-module` to the allow list. For more information, see File and Process Allow List in the *Nessus Agent User Guide*.

- Tenable Agents upgraded via Tenable Nessus Manager cannot upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions continue to use the cloud.tenable.com domain.

    - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.

- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.3.0 Release Notes - 2022-11-17

> **Note:** There is a known issue where upgrading and downgrading a Windows agent within a short period of time could cause the agent to become unresponsive. Tenable recommends that you do not upgrade or downgrade an individual Windows agent more than once every two hours. Doing so can cause `nessus-service` to stop. If this happens, restart the agent to restore `nessus-service`.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.3.0:

- Added support for the following operating systems:

    - macOS 13

    - Rocky Linux 8 and 9

    - AlmaLinux 8 and 9

- Tenable Agent now supports FIPS mode communications.

Upgrade Notes

- You can upgrade to the latest version of Tenable Agent from any previously supported version.

- If your upgrade path skips versions of the Tenable Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked Tenable Agents communicate with.
  - Tenable Vulnerability Management-linked Tenable Agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. If agents versions 8.1.0 through 10.3.1 are not able to connect to the new domain, they fall back to using cloud.tenable.com. Tenable Agent 10.3.2 and later do not fall back using the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Contact your network administrator for assistance with making necessary changes to your allow list.

Nessus Agent 10.3.1 Release Notes - 2022-12-12

Note: There is a known issue where upgrading and downgrading a Windows agent within a short period of time could cause the agent to become unresponsive. Tenable recommends that you do not upgrade or downgrade an individual Windows agent more than once every two hours. Doing so can cause `nessus-service` to stop. If this happens, restart the agent to restore `nessus-service`.

Bug Fixes

Bug Fix	Defect ID
Updated Nessus Agent to prevent excessive small reads that caused CPU spikes on Windows job requests.	5003a00001Ir3sNAAR, 5003a00001IG3MLAA1, 5003a00001IrA8IAAF
Updated Nessus Agent so that plugin updates do not affect	5003a00001IIHQiAAP

triggered scans during scan upload.	
Updated Nessus Agent to verify that the agent is running in a GCP environment before connecting to GCP metadata servers.	5003a00001IruKCAAZ, 5003a00001ItvB1AAJ

Upgrade Notes

- You can upgrade to the latest version of Tenable Agent from any previously supported version.
- If your upgrade path skips versions of the Tenable Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.
- If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked Tenable Agents communicate with.
    - Tenable Vulnerability Management-linked Tenable Agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. If agents versions 8.1.0 through 10.3.1 are not able to connect to the new domain, they fall back to using cloud.tenable.com. Tenable Agent 10.3.2 and later do not fall back using the cloud.tenable.com domain.
    - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Contact your network administrator for assistance with making necessary changes to your allow list.

2021 Tenable Agent

Nessus Agent 8.2.3 Release Notes - 2021-03-18

Nessus Agent 8.2.4 Release Notes - 2021-04-08

Nessus Agent 8.2.5 Release Notes - 2021-06-15

Nessus Agent 8.3.0 Release Notes - 2021-06-29

Nessus Agent 8.3.1 Release Notes - 2021-09-07

Nessus Agent 10.0.0 Release Notes - 2021-11-17

Nessus Agent 10.0.1 Release Notes - 2021-12-15

Nessus Agent 8.2.3 Release Notes - 2021-03-18

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Agent 8.2.3:

- **Hardware Support Updates** - In our ongoing efforts to support more hardware platforms, we have extended Nessus Agent support for the following:
  - Apple M1 Processor
- **Support for AWS EC2 IMDSv2** - Agents leveraged in AWS EC2 now support Instance Metadata Service version 2 (IMDSv2) for metadata collection where available. For EC2 instances that do not have IMDSv2 enabled, IMDSv1 will still be used for metadata collection.

For more information about the features and functionality supported in this release, see the Tenable Agent 8.2.x User Guide.

Bug Fixes

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Bug Fix	Defect ID
Resolved an issue where Agent service would be marked as an executable in some Linux installs.	01132263

Resolved an issue where Agents were sometimes showing an incorrect status when unable to authenticate to Nessus Manager.	01155311

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list..
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.
- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:
  - By default, the Agent update plan is set to update to the generally available (GA) version.
  - If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).

  - If you want your Agent to automatically update to the newest version, set your Agent update plan to `ea`.

- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:
  - Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.
  - To manually downgrade a Nessus Agent to a previous version (7.7.0 or greater), first disable automatic updates, then obtain the Agent package from Tenable Support and install it over your current version.

Nessus Agent 8.2.4 Release Notes - 2021-04-08

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Nessus Agent 8.2.4:

- OpenSSL was updated to the latest version 1.1.1k. For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.

  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.

  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list..

- You can upgrade to the latest version of Nessus Agent from any previously supported version.

- If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:

  - By default, the Agent update plan is set to update to the generally available (GA) version.

  - If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).

  - If you want your Agent to automatically update to the newest version, set your Agent update plan to `ea`.

- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:

  - Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.

  - To manually downgrade a Nessus Agent to a previous version (7.7.0 or greater), first disable automatic updates, then obtain the Agent package from Tenable Support and install it over your current version.

Nessus Agent 8.2.5 Release Notes - 2021-06-15

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Security Updates

The following are security updates included in Nessus Agent 8.2.5:

- This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 8.3.0 Release Notes - 2021-06-29

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Nessus Agent 8.3.0:

- Added a NessusCLI command to prepare Nessus Agents for imaging of the host system.
- Nessus Agents will now automatically detect damage to critical databases and restore them, without user interaction, reducing instances of Agents going offline due to environmental issue.
- Updated Agent DB compilation logic to ensure that the total Agent disk footprint is not expected to exceed 2GB.

Security Updates

The following are security updates included in Nessus Agent 8.3.0:

- This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Bug Fixes

- Resolved an issue where Agents installed on Windows 10 would show offline in Tenable Vulnerability Management after an automatic version update.
- Resolved an issue where Agent tags would be generated at install time instead of link time.
- Resolved an issue where nasl.exe missing due to AV would prevent Agents from upgrading.

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
    - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
    - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list..
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 8.3.1 Release Notes - 2021-09-07

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Nessus Agent 8.3.1:

- Operating System support for Fedora 33 and 34.
- Support for OpenSSL 1.1.1l.

For more information about the features and functionality supported in this release, see the Nessus Agent user guide.

Security Updates

This release includes fixes for potential vulnerabilities. For more information, see the following Tenable Product Security Advisory:

- https://www.tenable.com/security/tns-2021-15

Bug Fixes

Bug Fix	Defect ID
Resolved an issue where Agent would incorrectly identify itself as a source for jamalloc software updates in some Linux installs.	01195286
Resolved an issue where Agent would report an incorrect error code for an unlinked agent.	01200542

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.0.0 Release Notes - 2021-11-17

New Features

The following are the new features included in Tenable Agent 10.0.0:

- **Web Proxy Auto Detection for Windows** - Agents installed on Windows-based hosts may now use WPAD for web proxy, enabling Agents to adopt new configurations as the host connects to different networks.
- **Reduced Agent Footprint** - Agents now leverage an updated plugin compilation mechanism that creates a smaller footprint when installed on a host.
- **Support for Tenable Vulnerability Management feature coming in late Q4 2021: Regular Agent Information Updates in Tenable Vulnerability Management** - Agents will be able to update Tenable Vulnerability Management with their host asset information whenever a change is detected, regardless of their last scan completion, and provide a more up-to-date understanding of asset configurations.
- **Support for Tenable Vulnerability Management feature coming in Q1 2022: Rule-based Agent Scanning in Tenable Vulnerability Management** - Agent scans will be able to be configured using scan triggers, providing an alternative scanning model to the traditional scan window. Rule-based scan policies will be able to include multiple triggers. Agents will be able to initiate scans based on the triggers listed below. Rule-based scanning will be available for all Tenable Vulnerability Management Agents, including Tenable Security Center cloud Agents managed through Tenable Vulnerability Management.
    - *Time Interval* - Initiate Agent scans based on a user-defined time interval, regardless of the Agent's connectivity to Tenable Vulnerability Management, and upload the results the next time the Agent successfully connects.
        - Provides coverage for assets that may not be continuously connected to Tenable Vulnerability Management, returning the latest vulnerability results upon Agent check-in.
        - Enables better coverage for ephemeral assets, as Agents will check their policy on startup or boot. If the interval has ended, Agent will run a scan and upload the results to Tenable Vulnerability Management.

- *Filename* - Initiate Agent scans by placing an empty file, with a user-specified filename, into an assigned directory.
    - Enables integration with other tools.
    - Enables local admins to easily start a scan upon updating or patching a host system.
    - Files are placed in a `triggers` directory based on operating system:

Operating System	Directory
Windows	`/opt/nessus_agent/var/nessus/triggers`
Linux	`C:\ProgramData\Tenable\Nessus Agent\nessus\triggers`
macOS	`/Library/NessusAgent/run/var/nessus/triggers`

- *Ad-Hoc Local* - Initiate Agent scans locally via the Nessus CLI.
    - Enables local admins to easily start a scan upon updating or patching a host system.
    - Enabled by default for all rule-based scan policies.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.0.0:

- Operating System support for:
    - Fedora 35
    - Windows Server 2022
    - Windows 11
    - MacOS 12
    - Ubuntu 18.04 ARM

For more information about the features and functionality supported in this release, see the Nessus Agent user guide.

Security Updates

This release includes fixes for potential vulnerabilities. For more information, see the following Tenable Product Security Advisory:

Bug Fixes

Bug Fix	Defect ID
Resolved an issue where certain Windows AWS instances would not populate AWS metadata in Tenable Vulnerability Management.	n/a

Upgrade Notes

- Tenable Agents upgraded via Tenable Nessus Manager will not upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

Nessus Agent 10.0.1 Release Notes - 2021-12-15

New Features

The following are the new features included in Tenable Agent 10.0.1:

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Agent 10.0.1:

Security Updates

This release includes fixes for potential vulnerabilities. For more information, see the following Tenable Product Security Advisory:

Bug Fixes

Bug Fix	Defect ID
Resolved an issue where Tenable Agent was unable to complete scans on Windows hosts using certain international languages.	5003a00001BTn2vAAD

Upgrade Notes

- Tenable Agents upgraded via Tenable Nessus Manager will not upgrade to 8.2.0 and later unless Tenable Nessus Manager is already updated to 8.12.0 or later.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
    - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.

- **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding `*.cloud.tenable.com` (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of the Agent, Tenable recommends reviewing the release notes for all skipped versions to learn about new features and bug fixes.

2020 Tenable Agent

Nessus Agent 7.5.1 Release Notes - 2020-01-07

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following are the features included in Nessus Agent 7.5.1:

- Removed the requirement for upgrading to the latest version of Visual C/C++ runtime
- A new configuration setting was added to completely disable core updates for Nessus Agent. To enable this feature, in the Nessus Agent CLI, set `disable_core_updates` to `yes`. This disables the agent receiving automatic core updates from Tenable Vulnerability Management or Nessus Manager. Customers can still upgrade the agent directly via the installer.

Bug Fixes

Bug Fix	Defect ID
Removed the requirement for upgrading to the latest version of Visual C/C++ runtime	00936684

Upgrade Notes

If a Windows system was upgraded to Nessus Agent 7.5.0 and cannot start due to the Visual C/C++ runtime not being installed, you must upgrade to Nessus Agent 7.5.1 manually using the MSI installer.

> **Note:** If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.6.0 Release Notes - 2020-03-09

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

> **Note:** Nessus Agent 7.6.0 was re-released as Nessus 7.6.1 to address situations where an upgrade from an earlier version to Agent 7.6.0 did not complete due to an incomplete or corrupted download of the update package. This issue affected a small percentage of Nessus Agents connected to Tenable Vulnerability Management.

New Features

The following are the new features included in Nessus Agent 7.6.0:

- **Amazon Linux 2 Support** - Nessus Agents now support Amazon Linux 2 as a host operating system.

Changed Functionality and Performance Enhancements

The following are changes to functionality included in Nessus Agent 7.6.0:

- **Added MD5 check for the downloaded Nessus Agent core upgrade file** - Validate the integrity of the downloaded Nessus Agent software core by comparing its MD5 checksum to the value posted in the feed.
- **Added mechanism for Windows Agent nessus-service to better handle nessusd failure** - Prevent nessus_service on Windows from constantly restarting nessusd process. After a fixed number of restart attempts, nessus_service will stop. Must restart nessus-service after the upgrade to take advantage of this enhancement.

  For more information about the features and functionality supported in this release, see the Tenable Agent 7.6.x User Guide.

Bug Fixes

Bug Fix	Defect ID
Fixed issue where the backend.log is filled with sleep messages when an agent is unlinked.	00798667

Nessus Agent 7.6.1 Release Notes - 2020-03-11

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

- This release is a re-release of Nessus Agent 7.6.0 to address situations where an upgrade from an earlier version to Agent 7.6.0 did not complete due to an incomplete or corrupted download of the update package. This issue affected a small percentage of Nessus Agents connected to Tenable Vulnerability Management.

Upgrade Notes

- For those instances where the Nessus Agent service does not run, this may be due to a corrupted or incomplete `nessusd` executable. If this is the case, a manual install of the Nessus Agent may be required. If the Nessus Agent is running normally, this upgrade will simply ensure all files are at the same version.

Nessus Agent 7.6.2 Release Notes - 2020-04-21

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: For some customers on Nessus Agent 7.6.2, there was an issue when linking to Tenable Vulnerability Management via proxy. This was fixed in version 7.6.3.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where executing agent status commands would return an incorrect agent status error code.	00978397
Fixed an issue where some Nessus 7.5.x Agents on certain CentOS6/RH6 systems did not start correctly.	00947695, 00958001
Fixed an issue where some Nessus Agents running on Windows would fail with an exception when reading values from the registry.	00979447
Fixed an issue where Nessus Agent caused CPU usage to spike when it couldn't complete a plugin update due to the system being out of disk space.	00968303

Upgrade Notes

Note: If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.6.3 Release Notes - 2020-04-28

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Agent 7.6.3:

- OpenSSL is updated to version 1.1.1g to address a security patch in OpenSSL.

Bug Fixes

Bug Fix	Defect ID
Addressed an issue where Agent would not link to Tenable Vulnerability Management through a proxy when using cloud.tenable.com as the host	01015958

Upgrade Notes

Note: If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.7.0 Release Notes - 2020-06-09

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Agent 7.7.0:

- **AWS Graviton2 support** - Added support for Amazon Linux 2 on the AArch64 ARM-based architecture, which allows customers to run Agents on ARM platforms, including AWS Graviton2.
- **Update plan choice** - For Tenable Vulnerability Management-linked agents, users can set an update plan that determines the version that the agent automatically updates to. The options are as follows:

    - **Update to the latest GA release:** Update to the latest version as soon as it is made generally available (GA).
    - **Opt in to Early Access releases:** Update to the latest version as soon as it is released for Early Access (EA), typically a few weeks before general availability.
    - **Delay updates, staying on an older release:** Remain on an earlier version of Nessus Agent set by Tenable, which is at least one release older than the current generally available version. When Agent releases a new version, your instance updates software versions, but stays on a version prior to the latest release.

        > **Note:** Agent cannot downgrade to versions earlier than 7.7.0, so the agent remains on a minimum version of 7.7.0 if you set the update plan to delay updates.

    For more information, see Agent Update Plan in the *Nessus Agent User Guide*.

- **Downgrade support** - Added support for users to downgrade their agents to an earlier release.

    > **Note:** Agent cannot downgrade to versions earlier than 7.7.0.

    For more information, see Downgrade Nessus Agent in the *Nessus Agent User Guide*.

- **Duplicate Agent detection** - Checking for duplicate agents being created by cloned hosts, including logging of detections and a new setting to enable automatic re-identification of agents detected as duplicates. For more information, see Advanced Settings in the *Nessus Agent User Guide*.

Changed Functionality and Performance Enhancements

The following functionality was added or updated in Agent 7.7.0:

- DB settings updated for Agent Preferences DB, to reduce risk of DB corruption during heavy load.
- Better logging to track Agent software updates for Tenable Vulnerability Management-linked scanners.

Bug Fixes

Bug Fix	Defect ID

Fixed an issue where an Agent status query on certain non-English Windows systems incorrectly reported that the Agent was not running.	01010001

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 8.0.0 Release Notes - 2020-08-12

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

> **Note:** Tenable recommends upgrading to Tenable Agent 8.1.1 or Tenable Agent 8.2.0, which includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

New Features

The following are the new features included in Agent 8.0.0:

- **Upgrade Nessus Agent to latest version of Nessus Engine** - Incorporating the latest version of Nessus Engine to ensure functional parity and enable maintenance across Tenable scanning products. Users may notice that some Agent scans complete more quickly. Disk utilization is also increased on Linux platforms, due to the inclusion of additional plugins.
- **Updated Agent Status Command** - The `nessuscli agent status` command has been updated to provide more information about the current connection and scanning status of the Agent.

  > **Note:** The update to this command includes a modification of the output format. While this modification was designed to be backwards compatible, any users leveraging automation that utilizes this command should verify the output prior to upgrading.

  For more information, see Nessus CLI Agent Commands in the *Nessus Agent User Guide*.

- **Backup and Restore Tool** - Ability to create Agent backups that can easily and quickly be restored.

  > **Note:** For Windows users, the Agent uninstall process automatically creates a backup file in the %TEMP% directory. If you reinstall the Agent within 24 hours, the Agent uses that backup file to restore the installation. If you want to reinstall the Agent within 24 hours without using the backup, manually delete the backup file in the %TEMP% directory beforehand.

  For more information, see Back Up Agent and Restore Agent in the *Nessus Agent User Guide*.

- **Reminder: Downgrade support** - Agent 7.7.0 added support for users to downgrade their agents to an earlier release. Agent 8.0.0 will be the first time users will be able to leverage this functionality, if needed.

  > **Note:** Agent cannot downgrade to versions earlier than 7.7.0.

  For more information, see Downgrade Nessus Agent in the *Nessus Agent User Guide*.

Changed Functionality and Performance Enhancements

The following functionality was added or updated in Agent 8.0.0:

- Added log rotation for the nessusd.dump log file, including user-configurable settings to control rotation. For more information, see Advanced Settings in the *Nessus Agent User Guide*.
- Error checking to prevent incomplete file updates when Nessus Agent runs out of disk space.
- The advanced settings `ssl_mode` and `ssl_cipher_list` are now available for communication from Nessus Agents to other systems. For more information, see Advanced Settings in the *Nessus Agent User Guide*.

Upgrade Notes

- You can upgrade to the latest version of the Nessus Agent from any previously supported version.
- If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:
  - By default, the Agent update plan is set to update to the generally available (GA) version .
  - If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).
  - If you want your Agent to automatically update to the newest version, set your Agent update plan to `ea`.
- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:
  - Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.
  - To manually downgrade Nessus Agent from 8.0.0 to 7.7.0, first disable automatic updates, then obtain the Agent 7.7.0 package from Tenable Support and install it over your current version.
- On Ubuntu and other Debian-based Linux distributions, when doing a manual upgrade to Agent 8.0.0 from a prior version, the Agent service will remain stopped until explicitly started.

Nessus Agent 8.1.0 Release Notes - 2020-09-08

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: Tenable recommends upgrading to Tenable Agent 8.1.1 or Tenable Agent 8.2.0, which include a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

New Features

The following are the new features included in Agent 8.1.0:

- **Configure Scan and Plugin Compilation Performance and CPU Usage** - Using the nessuscli, users can set the performance mode separately for scans and for plugin compilation, which affects the amount of CPU utilized by the Nessus Agent during those processes. Users can set performance to high (default), medium, or low. Low performance slows down scans or plugin compilation, but reduces the agent's CPU consumption. Setting the performance to medium or high means that scans or plugin compilation completes more quickly, but the agent consumes more CPU. For more information about `plugin_load_performance_mode` and `scan_performance_mode`, see Advanced Settings in the Nessus Agent User Guide.

Changed Functionality and Performance Enhancements

The following functionality was added or updated in Agent 8.1.0:

- Added extended operating system and library dependency checking to ensure Nessus Agents that update automatically meet the necessary dependencies as a prerequisite to upgrading.

Bug Fixes

Bug Fix
Resolved an issue with Debian based install packages where the Agent service did not automatically restart after upgrade.

Upgrade Notes

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures

communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list.

- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.
- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:
  - By default, the Agent update plan is set to update to the generally available (GA) version .
  - If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).
  - If you want your Agent to automatically update to the newest version, set your Agent update plan to `ea`.
- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:
  - Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.
  - To manually downgrade a Nessus Agent to a previous version (7.7.0 or greater), first disable automatic updates, then obtain the Agent package from Tenable Support and install it over your current version.

Agent 8.1.1 Release Notes - 2020-11-04

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Upgrade Notes

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
    - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
    - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list..
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.
- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:
    - By default, the Agent update plan is set to update to the generally available (GA) version .
    - If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).
    - If you want your Agent to automatically update to the newest version, set your Agent update plan to ea.
- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:

- Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.

- To manually downgrade a Nessus Agent to a previous version (7.7.0 or greater), first disable automatic updates, then obtain the Agent package from Tenable Support and install it over your current version.

Nessus Agent 8.2.0 Release Notes - 2020-10-29

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Agent 8.2.0:

- **Staggered Scan Start** - Users can now set a staggered scan start time for agent scans in Tenable Vulnerability Management and Nessus Manager. Agents deployed in that scan will delay starting the scan for a random number of minutes up to the maximum delay time set by the user. This is helpful in reducing load in environments with shared resources, such as virtual machine CPU, because agents will not all begin scanning at once.

  > **Note:** Nessus 8.12.0 or later is required to leverage this functionality in Nessus Manager.

  For more information, see Advanced Scan Settings in the *Tenable Vulnerability Management User Guide* or Advanced Scan Settings in the *Tenable Nessus User Guide* .

- **OS Support Updates** - In our ongoing efforts to support as many operating system variants as possible for our customers, we have extended Nessus Agent support for the following operating systems:

  - Ubuntu 20.04

  - SUSE Enterprise Server 15

  - Kali Linux 2018, 2019 & 2020

Changed Functionality and Performance Enhancements

The following functionality was added or updated in Agent 8.2.0:

- **Operating System & Library Pre-Upgrade Checks** - Nessus Agent will now check that the host system is running a supported operating system version as well as any required libraries before upgrading to a new Agent version. For more information on supported operating systems, see Software Requirements in the *Tenable Agent Deployment and User Guide*.
- **Windows Dependency Update** - Nessus Agent 8.2.0 and later requires Windows host systems to be running the Universal Microsoft C Runtime Library (UCRT) (for more information, see Microsoft Documentation). This means that some older versions of Microsoft Windows will require a minimum update to work with Nessus Agent 8.2.0 and later. Current Windows Agent installations that do not meet these requirements will not automatically upgrade past Agent 8.1.0.

  The following lists the Windows variants and their minimum upgraded state. Users should experience no functional difference as a result of this change.

  - Windows 7 SP1
  - Windows 8.1 with April 2014 update
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2
  - Windows Server 2012R2 with April 2014 update

Bug Fixes

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Bug Fix	Defect ID
Resolved an issue where Windows Agents could potentially use excessive CPU in a socket failure scenario.	01077419
Resolved an issue where reinstalling a new Agent was unexpectedly restoring the backup from a previously uninstalled agent version.	01062064

Added a timeout for Windows WMI calls within Agent scans, to prevent scans from stalling if the WMI API never returns.	00997983
Resolved an issue where some Windows systems were experiencing java.exe being deleted if it existed in the Agent startup directory	01084260

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list..
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.
- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:

    - By default, the Agent update plan is set to update to the generally available (GA) version .
    - If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).
    - If you want your Agent to automatically update to the newest version, set your Agent update plan to `ea`.
- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:
    - Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.
    - To manually downgrade a Nessus Agent to a previous version (7.7.0 or greater), first disable automatic updates, then obtain the Agent package from Tenable Support and install it over your current version.

Nessus Agent 8.2.1 Release Notes - 2020-11-24

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following are the new features included in Agent 8.2.1:

- **OS Support Updates** - In our ongoing efforts to support as many operating system variants as possible for our customers, we have extended Nessus Agent support for the following operating systems:
    - macOS 11.0 Big Sur
    - Fedora 31 & 32

Bug Fixes

Bug Fix	Defect ID
Resolved an issue where Nessus Agent was not failing back to cloud.tenable.com in the event sensor.cloud.tenable.com wasn't available without restarting the Nessus Agent service.	01111764

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.

- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.

  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.

  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list..

- You can upgrade to the latest version of Nessus Agent from any previously supported version.

- If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:

- By default, the Agent update plan is set to update to the generally available (GA) version .
- If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).
- If you want your Agent to automatically update to the newest version, set your Agent update plan to `ea`.

- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:
  - Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.
  - To manually downgrade a Nessus Agent to a previous version (7.7.0 or greater), first disable automatic updates, then obtain the Agent package from Tenable Support and install it over your current version.

Nessus Agent 8.2.2 Release Notes - 2020-12-15

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following are changed functionality in Agent 8.2.2:

- Nessus Agent now leverages OpenSSL version 1.1.1i.

Bug Fixes

Bug Fix	Defect ID
Resolved an issue where a manual package upgrade on debian-based Linux installers could result in the agent not restarting properly.	01118278

Upgrade Notes

- Users upgrading agents via Nessus Manager will not upgrade to 8.2.0 and later unless Nessus Manager is already updated to 8.12.0 or higher.
- **New Tenable Vulnerability Management Domain** - As a part of continuous security and scalability improvements to Tenable infrastructure, we have added a new sensor.cloud.tenable.com domain that Tenable Vulnerability Management-linked agents communicate with.
  - Starting with Agent 8.1.0, Tenable Vulnerability Management-linked agents communicate with Tenable Vulnerability Management using sensor.cloud.tenable.com. In case agents are not able to connect to the new domain, they fall back to using cloud.tenable.com. Agents with earlier versions will continue to use the cloud.tenable.com domain.
  - **Recommended Action:** If you use domain allow lists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allow list. This ensures communication with sensor.cloud.tenable.com and all future subdomains, reducing operational overhead. Please contact your network administrator for assistance with making necessary changes to your allow list..
- You can upgrade to the latest version of Nessus Agent from any previously supported version.
- If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.
- Tenable Vulnerability Management-linked Agents now support the ability to choose your Agent update plan:
  - By default, the Agent update plan is set to update to the generally available (GA) version .
  - If you want to manually update your Agents to the newest version when it is made available for Early Access (EA), first disable automatic updates so the agent does not automatically downgrade to the previous version (GA).
  - If you want your Agent to automatically update to the newest version, set your Agent update plan to ea.
- Nessus Agents 7.7.0 and later support the capability to downgrade from a later version:

- Tenable Vulnerability Management-linked Nessus Agents support automatically downgrading via the Agent update plan setting. To automatically revert a Tenable Vulnerability Management-linked Nessus Agent to the previous version, set your Agent update plan to `stable`. Your agent will always remain on an earlier version than the latest GA version until you change your update plan.
- To manually downgrade a Nessus Agent to a previous version (7.7.0 or greater), first disable automatic updates, then obtain the Agent package from Tenable Support and install it over your current version.

2019 Tenable Agent

Nessus Agent 7.3.0 Release Notes - 2/26/2019

Nessus Agent 7.3.1 Release Notes - 2019-03-26

Nessus Agent 7.3.2 Release Notes - 2019-04-17

Nessus Agent 7.4.0 Release Notes - 2019-05-07

Nessus Agent 7.4.1 Release Notes - 2019-06-25

Nessus Agent 7.4.2 Release Notes - 2019-08-13

Nessus Agent 7.4.3 Release Notes - 2019-09-24

Nessus Agent 7.5.0 Release Notes - 2019-12-12

Nessus Agent 7.3.0 Release Notes - 2/26/2019

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- Agent CPU Prioritization - This feature will allow customers to set the relative CPU priority of the Nessus Agent and set all child processes (Priority not inherited in Windows on elevated status) via the nessuscli. The user can set the priority to standard, lowered priority, and elevated priority, with standard priority being the default. This will affect the speed at which a scan completes as well.

Bug Fix

- Fixed a bug that would relink the agent to Tenable Vulnerability Management using its hostname rather than a previously configured custom name during the migration of a Nessus Agent from Tenable Nessus Manager to Tenable Vulnerability Management.

Upgrade Notes

- Prior to deploying the GA version of 7.3.0, the EA version must be uninstalled.

> **Note:** If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.3.1 Release Notes - 2019-03-26

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality

- Improved agent check-in logic to improve reliability of agent scan result uploads
- Improved support for unicode characters in scan reports

Bug Fixes

- Resolved an issue where an agent running on an AWS EC2 M5 instance would not report that it was running in AWS EC2
- Resolved an issue where agent scan results would not upload under certain conditions.
- Resolved an issue with the RPM installers stopping all nessusd processes on the host (Only a problem if both Nessus Scanner and Tenable Agent are installed).

  > **Note:** Operating systems that use the RPM installer should upgrade via the RPM package to receive this latest RPM fix. Upgrading an RPM installation via the feed will leave the RPM associated with that agent on the host.

Upgrade Notes

- Prior to deploying the GA version of 7.3.1, the EA version must be uninstalled.

> **Note:** If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.3.2 Release Notes - 2019-04-17

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Fixed an issue with Agent uploads where scan results could be lost for large deployments.
- Fixed an issue with a scan status being out of sync between Agents and Tenable Vulnerability Management or Nessus Manager resulting in aborting result uploads for large deployments.
- Fixed an issue with scan result upload scheme resulting in unsustainable load for Tenable Vulnerability Management.

Nessus Agent 7.4.0 Release Notes - 2019-05-07

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Fixed a bug that caused the nessuscli command with the `--cloud` argument to always return success, even in the event of a failure.

Nessus Agent 7.4.1 Release Notes - 2019-06-25

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

- Fixed a bug, where corrupted plugins would not reload. In this case, Nessus Manager's backend.log file would incorrectly report a "Failed to load scan" message.

Upgrade Notes

- Prior to deploying the GA version of Nessus Agents 7.4.1, the EA version must be uninstalled.

> **Note:** If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.4.2 Release Notes - 2019-08-13

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- Agent startup delay - In order to ease initial deployment of large numbers of agents, Tenable has built in a variable startup delay for Nessus Agents of 0-300 seconds

Changed Functionality and Performance Enhancements

- Updated version of OpenSSL - The Nessus Agent now uses version 1.0.2s

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where agents running on some Mac OSes did not restart after a reboot	00477343

Upgrade Notes

- **Note:** If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.4.3 Release Notes - 2019-09-24

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

- **RHEL 8 Support:** The Nessus Agent now supports Red Hat Enterprise Version 8.

Bug Fixes

Bug Fix	Defect ID
Fixed a bug where Nessus Agents running on AWS PV instance types did not return metadata.	00825664
Fixed a bug where Nessus Agents did not know they were unlinked from Tenable Vulnerability Management and Nessus Manager.	00783468

Upgrade Notes

- **Note:** If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Nessus Agent 7.5.0 Release Notes - 2019-12-12

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following is a new feature included in Nessus Agent 7.5.0:

- **MAC Catalina (10.15) Support** - Nessus Agents now support MAC Catalina as a supported host operating system.

Changed Functionality and Performance Enhancements

- **Open SSL v1.1.1 Update** - Nessus Agents will leverage OpenSSL v1.1.1 as part of this release.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where Agents were unlinking during re-installation.	00801887
Fixed an issue where Agents were unlinking after a scan.	00894457
Fixed an issue where Agents were disconnecting from Tenable Vulnerability Management.	00820918

Upgrade Notes

Note: Nessus Agent 7.5.0 required the installation of Visual C++ Redistributable for Visual Studio 2015 on the host operating system. Tenable Agent 7.5.1 removes that requirement.

For Nessus Agents 7.5.0 running on Windows, you must install Visual C++ Redistributable for Visual Studio 2015 on the host operating system. Some versions of Windows require that you install the latest service pack and/or security patch before you can install Visual C++ Redistributable for Visual Studio 2015. The following are the affected operating systems:

- Windows Server 2008 (requires SP2)
- Windows Server 2008 R2 (requires SP1)
- Windows 7 (requires SP1)
- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

For more information, see the knowledge base article.

Note: If your upgrade path skips versions of Nessus Agents, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

2018 Tenable Agent

Nessus Agent 7.0.1 Release Notes - 1/11/2018

Nessus Agents 7.0.3 Release Notes - 3/14/2018

Nessus Agent 7.1.0 Release Notes - 6/13/2018

Nessus Agent 7.1.1 Release Notes - 8/14/2018

Nessus Agent 7.1.2 Release Notes - 11/05/2018

Nessus Agent 7.2.0 Release Notes - 12/17/2018

Nessus Agent 7.2.1 Release Notes - 12/20/2018

Nessus Agent 7.0.1 Release Notes - 1/11/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

File Names & MD5 Checksums

File	MD5
NessusAgent-7.0.1-amzn.x86_64.rpm	cdb717380ed440f23cd6b0c6a453ea42
NessusAgent-7.0.1-debian6_amd64.deb	fdd66af6828b524c190414ced4156e59
NessusAgent-7.0.1-debian6_i386.deb	0606ddd905e5320a70f32e630f402a3e
NessusAgent-7.0.1-es5.x86_64.rpm	80e2d2696ceb4f40ffe61e16b48f1ed8
NessusAgent-7.0.1-es5.i386.rpm	a13d8d379efae9b7becfa4c8228dc958

File	MD5
NessusAgent-7.0.1-es6.x86_64.rpm	cd798010aabe6d1c30a92f665f8a3993
NessusAgent-7.0.1-es6.i386.rpm	786595a792626bec85dcbebc41790ded
NessusAgent-7.0.1-es7.x86_64.rpm	91766d919a982d8df8ed0a0130255b63
Nessus-7.0.1-fbsd10-amd64.txz	a8a3a34ef22eb164d87a9a018905dd99
NessusAgent-7.0.1-fc20.x86_64.rpm	35d46ef591c4fb6d91605f750e32f27a
NessusAgent-7.0.1.dmg	95634e68b7c367926a5f7f7a8abc6c0b
NessusAgent-7.0.1-suse11.x86_64.rpm	9a031a3e67f718d7aa7a676c6b6ff5db
NessusAgent-7.0.1-suse11.i586.rpm	ec07edf476ed851d180d8a3f7409d435
NessusAgent-7.0.1-suse12.x86_64.rpm	a679d1ae6cf22797dfcddff70454f312
NessusAgent-7.0.1-ubuntu1110_amd64.deb	9bb099d9765f8361023087b5472cb2e7
NessusAgent-7.0.1-ubuntu1110_i386.deb	552c3b2130bd0a04514d6dcef0781e4e
NessusAgent-7.0.1-ubuntu910_amd64.deb	0325e32947663b792d4673e73689c85f
NessusAgent-7.0.1-ubuntu910_i386.deb	60b405742bccc5ce175329978f5c1bb8
NessusAgent-7.0.1-Win32.msi	82730052a7f4cf666206ca1c70c0462c
NessusAgent-7.0.1-x64.msi	f731d76ecb71a7acacb364ef0421b470

Nessus Agents 7.0.3 Release Notes - 3/14/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

What's new

- Proxy fallback to direct connection
- Auto-relinking for offline install support
- Windows system tray application

File Names & MD5 Checksums

File	MD5
NessusAgent-7.0.3-x64.msi	2dffed53708b9cc771ac5b80cf14696a
NessusAgent-7.0.3-amzn.x86_64.rpm	ab2cbd81bd47fa2a2cd4aaa276a92dce
NessusAgent-7.0.3-Win32.msi	07113eaa8487faa93ef43183d95570eb
NessusAgent-7.0.3-debian6_i386.deb	4ba0713554230510aeb11efa08e945d9
NessusAgent-7.0.3.dmg	cf454de571a54336af7fedc0d16d181b
NessusAgent-7.0.3-debian6_amd64.deb	cf52cc686dc1b68b03e2acdf2f7ab2bb
NessusAgent-7.0.3-es5.x86_64.rpm	adc5a33c0749d9b3f934805be76f49e0
NessusAgent-7.0.3-es5.i386.rpm	3808b79a5bec69369f829a6af45dea21
NessusAgent-7.0.3-es6.x86_64.rpm	574e3ea417a4ccb7a0c51247ea270c76
NessusAgent-7.0.3-es6.i386.rpm	6fd34a4f2461bc0a76766cccf598599f
NessusAgent-7.0.3-fc20.x86_64.rpm	6907b7e97d2551008cddd8ada93fc733
NessusAgent-7.0.3-es7.x86_64.rpm	cb4a6327955fd8826f330e9f945b6c31
NessusAgent-7.0.3-suse11.i586.rpm	ba6c6bf136d64077bd1573a1547319d1
NessusAgent-7.0.3-suse11.x86_64.rpm	8e0d3c241543d5c745149e34d2f68085
NessusAgent-7.0.3-ubuntu910_amd64.deb	25a3a8428c8c71069271822edd2951fc
NessusAgent-7.0.3-suse12.x86_64.rpm	a4e15c4f666363521881ea34c3ebf455
NessusAgent-7.0.3-ubuntu910_i386.deb	359ad78b3f48b7a9899beeb912d7a02a
NessusAgent-7.0.3-ubuntu1110_amd64.deb	ebcfd859fec622695bc9b35c056bed57
NessusAgent-7.0.3-ubuntu1110_i386.deb	8e613cccb62e6feebb492ac67b5862a4
nessus-agent-updates-7.0.3.tar.gz	36748d6719229cb68f1501aad33598a4

Nessus Agent 7.1.0 Release Notes - 6/13/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

What's new

Note: If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Note: Each of these new features require Nessus Manager 7.1.1.

- Automatically update the hostname of an agent in Nessus Manager when it changes. This feature allows the agent hostname to be updated automatically instead of requiring the agent to be unlinked and relinked. This requires the "update_hostname" parameter to be set to "yes".
- Export full list of agents via the Nessus Manager UI. This provides customers, who do not leverage the Nessus API, the ability to export the agent details as a .csv report for use.
- Track agents and attributes after unlinking. This provides users the ability to continue tracking unlinked agents and associated details. This is an opt-in feature.
- Automatically maintain unique agents in Nessus Manager. This eliminates situations where multiple entries for the same agent can appear in Nessus Manager.
- Updated third-party libraries with known vulnerabilities, see the security advisory for more information.

Bug Fixes and Improvements

- Fixed an issue where a database lock could occur in certain situations preventing agent scan results from being processed properly.
- Fixed an issue where the agent failed to link through a proxy when using the offline install feature.
- Fixed an issue where the Windows agent installer was not respecting the silent uninstall option.
- Updated OpenSSL to 1.0.2o.

- Updated PCRE to 8.42.
- Updated expat, libjpeg, Libxml2, libxslt, libxmlsec and zlib third-party libraries

File Names & MD5 Checksums

File	MD5
NessusAgent-7.1.0-amzn.x86_64.rpm	9cd6d109e1fb81f8debf74470a67cc20
NessusAgent-7.1.0-debian6_amd64.deb	8b4f042a68d0afba089b7ccb028c8b5e
NessusAgent-7.1.0-debian6_i386.deb	fd58687a9d14e9779f7fb7c34c0cedf1
NessusAgent-7.1.0-es5.x86_64.rpm	e3d4d0c0c869fcbed6c9d0e1fb3c3d07
NessusAgent-7.1.0-es5.i386.rpm	830050513e50f43a302f5d2d94e95300
NessusAgent-7.1.0-es6.x86_64.rpm	7b7ea00d23e9554360eca610808ad419
NessusAgent-7.1.0-es6.i386.rpm	b12a8286057809994be8f71b94b49a57
NessusAgent-7.1.0-es7.x86_64.rpm	216e26b6254fd2ba3c78c3fcd58e93f0
NessusAgent-7.1.0-fc20.x86_64.rpm	0a7ab76941df6d0b0035efcc9347f970
NessusAgent-7.1.0.dmg	b8c82973e86afe09512f9740cdecc186
NessusAgent-7.1.0-suse11.x86_64.rpm	8540d6e97a9ae7696ecab4b8e25d4738
NessusAgent-7.1.0-suse11.i586.rpm	1239aa20ba79ffb33d530b56efeb07f4
NessusAgent-7.1.0-suse12.x86_64.rpm	42ef400245e77d5dab85f3001a3a1d13
NessusAgent-7.1.0-ubuntu1110_amd64.deb	6eb03afaf326c902907b17ba356b0539
NessusAgent-7.1.0-ubuntu1110_i386.deb	127a9507a3348202c20d58633d0056bb
NessusAgent-7.1.0-ubuntu910_amd64.deb	cde44e3eeed2babadc421ea4c5740fc0
NessusAgent-7.1.0-ubuntu910_i386.deb	0ef3a9c0c38b8b8527938a3bed83e4ca
NessusAgent-7.1.0-x64.msi	ac7c1889766c6b19a0e23325b24705b5
NessusAgent-7.1.0-Win32.msi	2245a0a9719140ee1327d7740efbba42

Nessus Agent 7.1.1 Release Notes - 8/14/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

What's new

Note: If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

The following new features are included with Nessus Agent 7.1.1. Customers are not required to update Nessus Manager to take advantage of these features:

- Option to deploy plugins as part of the Agent Installation. Provides options to reference a plugin file during Agent installation to help reduce network strain when deploying Agents at scale.
- Automatically update the hostname of an agent in Tenable Vulnerability Management when it changes. This feature allows the agent hostname to be updated automatically instead of requiring the agent to be unlinked and relinked.
- Additional logging on local Agents. Provides better insight for administrators to help troubleshoot activity on the Agent.

Bug Fixes and Improvements

- Fixed an issue where differential plugin updates were inoperable for Tenable Vulnerability Management customers and thereby defaulting to full plugin updates across all Agents.
- Fixed an issue where Agent update versions were not being reflected correctly in the Windows registry.
- Fixed an issue where silent mode was prompting user for input if the install directory was present during installation.
- Fixed an issue where the Agent uninstallation did not delete all files and directories.

File Names & MD5 Checksums

File	MD5
NessusAgent-7.1.1-amzn.x86_64.rpm	68c86404a6f11f4203963b306603bee4
NessusAgent-7.1.1-debian6_amd64.deb	6d5c0b4c4268590076ba7bfb56a34e32
NessusAgent-7.1.1-debian6_i386.deb	3e86dc05b29892fc6d077ea0c81e7739
NessusAgent-7.1.1-es5.x86_64.rpm	d77b961faffb78ffb1c7810fa50608ad
NessusAgent-7.1.1-es5.i386.rpm	ec14317e20d4e25220f3239663ca9dda
NessusAgent-7.1.1-es6.x86_64.rpm	a7ddaf844013507465eb778b77f2221e
NessusAgent-7.1.1-es6.i386.rpm	5eae9c60ed832fde886ace38c8603844
NessusAgent-7.1.1-es7.x86_64.rpm	47573d68484a92c5d6bc2338922970fd
NessusAgent-7.1.1-fc20.x86_64.rpm	7f40154c014820c590758af2f4453b75
NessusAgent-7.1.1.dmg	a01058cd78717be61ca35290443e8daf
NessusAgent-7.1.1-suse11.x86_64.rpm	7dcb5d9c0efafadbcc7b8a2646d83b8c
NessusAgent-7.1.1-suse11.i586.rpm	1e9a086bd79a8674d39561e55e3a704d
NessusAgent-7.1.1-suse12.x86_64.rpm	6fd6e1530517fbff27b6291429612e96
NessusAgent-7.1.1-ubuntu1110_amd64.deb	477b6686f7631755e228be848dc295b2
NessusAgent-7.1.1-ubuntu1110_i386.deb	b4030ce03f74ae32617f132105deeb9f
NessusAgent-7.1.1-ubuntu910_amd64.deb	f3cbbee84ad5d5c70825980399fbb9a0
NessusAgent-7.1.1-ubuntu910_i386.deb	5a890d264365e563eb91c6d6ad48a777
NessusAgent-7.1.1-x64.msi	6f5237ef95114f22aa36afab89d4cf3b
NessusAgent-7.1.1-Win32.msi	f6c177054152c0434e4bc85c513115ea

Nessus Agent 7.1.2 Release Notes - 11/05/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

What's new

The following new features are included with Nessus Agent 7.1.2. Customers are not required to update Nessus Manager to take advantage of these features. Additional details on features are available in the Nessus Agent 7.1.2 User Guide.

- **Additional insight for administrators into offline agents:** Expanded details are now provided when running `nessuscli` on an agent for troubleshooting. Previously, no data was provided in cases where an agent wasn’t able to connect to Tenable Vulnerability Management. It’s now possible to see additional details such as agent state (running, not running), linked status, active scans and jobs pending, and last successful connection by running `nessuscli agent status` on an agent with the `--local` argument.
- **Automatic restart for Linux Agents after upgrading:** This enhancement streamlines the restart for agents which previously required an additional manual step during an upgrade.
- **Better visibility into agents running in EC2:** EC2 metadata is now provided in the agent logs during linking or upgrade activity.
- **Better resilience for agent retries:** You can set a maximum number of retries for agent when attempting to link to Tenable Vulnerability Management.
- **Added support for new operating systems:** Nessus Agents are now supported on macOS Mojave 10.14, Amazon Linux 2018.03, and Windows Server 2019.

Bug Fixes and Improvements

- Fixed an issue where core downloads failed to retry after one failure.
- Fixed an issue impacting connectivity for agents to Tenable Vulnerability Management in proxy environments.

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Caution: Nessus Agent version 7.1.1 might enter a state where it is unable to upgrade to Nessus Agent 7.1.2.

Upgrade options and instructions for Nessus Agents are available in the Nessus Agent 7.1.2 User Guide.

A 7.1.1 Nessus Agent might enter a state where it's prevented from applying a core update from 7.1.1 to a newer version, but still continue to receive plugin updates and run scans. The issue occurs when a plugin update (full or differential) and a core update are both available. The issue impacts any 7.1.1 agent that is managed by Nessus Manager and configured to automatically receive core and plugin updates. Agents managed by Tenable Vulnerability Management are not expected to experience the issue.

Agents will continue to receive plugins and run scans while in this state. The following options can be utilized to mitigate the issue and provide a way to upgrade impacted agents being managed by Nessus Manager.

- Nessus Manager Upgrade - Upgrade your Nessus Manager installation to a newer version. Nessus Manager 8.0.1 includes logic that will prevent the issue and allow 7.1.1 agents to upgrade. Alternatively, you can upgrade to Nessus Manager 7.2.2 which is targeted for release on November, 15th 2018.
- Manually upgrade the Nessus Agent on each asset.

If the two options above aren't feasible, you can recover from the loop with this workaround:

- Restart the agent or the asset that contains the agent. Upon restart, the agent will check-in, process the core update to 7.1.2, and resume as normal.

Tip: You can examine a Nessus Agent's `backend.log` file to determine if a Nessus Agent is in a restart loop. An example log that illustrates the issue is available here.

Additionally, the 7.1.2 EA version should be uninstalled prior to deploying the 7.1.2 GA version.

File Names & MD5 Checksums

For a full list of file names and checksums for this release, see the Tenable Downloads Page.

To get the MD5 and SHA256 checksums for a file, click **Checksum** in the **Details** column.

Nessus Agent 7.2.0 Release Notes - 12/17/2018

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Feature

- Customers using Nessus Manager must be running version 8.1.0 to take advantage of the log retrieval feature. Otherwise no upgrade is necessary on Nessus Manager.

Changed Functionality and Performance Enhancements

- **Improved troubleshooting capabilities for Agents** (Remote Log Extraction) - This feature allows administrators using Nessus Manager 8.1.0 and later to download logs from individual Agents via the Nessus Manager UI.

  > **Note:** This capability is only available for customers using Nessus Manager 8.1.0 and later to manage their agents.

- **Improved Unicode Support** - Windows Agents. This capability improves support for non-latin characters retrieved from Windows Agents
- **Continued Improvement For Agents Running in EC2.** Additional Metadata fields for agents running in EC2 are now provided:
  - mac address
  - iam/security-credentials/
  - iam/security-credentials/role-name
  - security-groups
  - public-keys/0/openssh-key

Bug Fixes

- Fixed an issue where the Nessus Agent would report its IP address as an APIPA address.
- When upgrading the Nessus Agent, the installer will remove unnecessary files within the Nessus Agent folder, which were causing an incorrect version to display.

Upgrade Notes

Note: If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Prior to deploying the GA version of 7.2.0, the EA version must be uninstalled.

Nessus Agent 7.2.1 Release Notes - 12/20/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fix

- This hotfix addresses an issue with Agents 7.2.0 that resulted in import/export issues with Tenable Security Center, Nessus Manager, and Tenable Vulnerability Management.

2017 Tenable Agent

Nessus Agent 6.10.2 Release Notes - 2/21/2017

Nessus Agent 6.10.3 Release Notes - 3/14/2017

Nessus Agent 6.10.4 Release Notes - 3/21/2017

Nessus Agent 6.10.5 Release Notes - 4/11/2017

Nessus Agent 6.10.6 Release Notes - 5/24/2017

Nessus Agent 6.10.7 Release Notes - 5/31/2017

Nessus Agent 6.10.8 Release Notes - 6/21/2017

Nessus Agent 6.10.9 Release Notes - 7/14/2017

Nessus Agent 6.11.0 Release Notes - 8/7/2017

Nessus Agent 6.11.1 Release Notes - 8/14/2017

Nessus Agent 6.11.2 Release Notes - 10/26/2017

Nessus Agent 6.11.3 Release Notes - 12/5/2017

Nessus Agent 7.0.0 Release Notes - 12/12/2017

Nessus Agent 6.10.2 Release Notes - 2/21/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.2-amzn.x86_64.rpm	dd91e1e877179bfb13198f19e97989e2
nessusagent-6.10.2-debian6_amd64.deb	07003fda6f25ac3cc3b444d8f0b70f86
nessusagent-6.10.2-debian6_i386.deb	352026c33003a5634dcc037d05efe956
nessusagent-6.10.2.dmg	5e82bf6215caa1a6683d6de1f777af4c
nessusagent-6.10.2-es5.i386.rpm	2cdb076570512c561cf172b43f90dfe9
nessusagent-6.10.2-es5.x86_64.rpm	5a8854923bd0c4623363b192045b9bb7
nessusagent-6.10.2-es6.i386.rpm	b71a8e7aa47a1065cd08bc77ef06aadc
nessusagent-6.10.2-es6.x86_64.rpm	61866bc0b65cba91dbf9adfdf318fc88
nessusagent-6.10.2-es7.x86_64.rpm	0a42d5838aac2e468663463e1133a6e3
nessusagent-6.10.2-fc20.x86_64.rpm	c1995cd2e7276155ac34ca70771404b5
nessusagent-6.10.2-suse11.i586.rpm	fbd14f900060fc45fd3f3ddd5bdbc3bf
nessusagent-6.10.2-suse11.x86_64.rpm	c5354ac8a5b728eb5d7a4abdb3831b93
nessusagent-6.10.2-suse12.x86_64.rpm	11f8bb500ff15e770d9420b39025482e
nessusagent-6.10.2-ubuntu1110_amd64.deb	9b5b955d4b14d85d272202ac85e82264
nessusagent-6.10.2-ubuntu1110_i386.deb	70496b39879ae9e5f1c9a708f8cb65a9
nessusagent-6.10.2-ubuntu910_amd64.deb	b4108bf59e2b5e053a2898b84e5a2484
nessusagent-6.10.2-ubuntu910_i386.deb	5428ab4e8f4c4ffb4c26175427207a8b

File	MD5
nessusagent-6.10.2-Win32.msi	73d096bd4f2495473180bbe161bf8903
nessusagent-6.10.2-x64.msi	95cfa585912c863252c34df98fd9c999

Nessus Agent 6.10.3 Release Notes - 3/14/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Require agents and managed scanners to respect controller sleep times

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.3-amzn.x86_64.rpm	50cd9be9a02d7ceb4fa1e89cbe374064
nessusagent-6.10.3-debian6_amd64.deb	219a14bb3451a53125df14c828e5c5a0
nessusagent-6.10.3-debian6_i386.deb	692369bd268ae907b29047328e612780
nessusagent-6.10.3.dmg	e5de4ab45e0cb04d07d5266bee629c71
nessusagent-6.10.3-es5.i386.rpm	5c8304201583df442494615987791be4
nessusagent-6.10.3-es5.x86_64.rpm	f33e777f345dbc1fbc7d075b5d73b90f
nessusagent-6.10.3-es6.i386.rpm	659abf08182d07d6296588f87c6d97d9
nessusagent-6.10.3-es6.x86_64.rpm	f3651114d45d0fc129bfc5e3215cfd9e
nessusagent-6.10.3-es7.x86_64.rpm	e62ee0cefc3ee1c80fa43ca2f933c85d
nessusagent-6.10.3-fc20.x86_64.rpm	c649a2c290877e5b5859c751168eb2eb
nessusagent-6.10.3-suse11.i586.rpm	5ae7aaff4a4069ec44d3bdd32ad5bbef
nessusagent-6.10.3-suse11.x86_64.rpm	c41fbf7bf07726001c78f97b2ff42318
nessusagent-6.10.3-suse12.x86_64.rpm	e2ddcc0c2fa4b6d2a71a164001a4fa7a
nessusagent-6.10.3-ubuntu1110_amd64.deb	7320b6e53fda8e006867d829514e3b12

File	MD5
nessusagent-6.10.3-ubuntu1110_i386.deb	fd7731015e89cad67d950fb6c92590d4
nessusagent-6.10.3-ubuntu910_amd64.deb	19f331aa18c845855a3f8e8119b11a6e
nessusagent-6.10.3-ubuntu910_i386.deb	ce25024bbecc7b8d4d884370818ce2fd
nessusagent-6.10.3-Win32.msi	386cb125d8d2d20600a605bdb6e01004
nessusagent-6.10.3-x64.msi	04685304445c27e446d582751b47ed6b

Nessus Agent 6.10.4 Release Notes - 3/21/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Fix to enforce permissions on the plugins folder in agent mode
- Prevent attempts for agent to scan if plugins are not installed

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.4-amzn.x86_64.rpm	0c838b9580f245a49bb2582f55e204d8
nessusagent-6.10.4-debian6_amd64.deb	ff4ab7aa7ba155c4c0aae7ef50b03dc3
nessusagent-6.10.4-debian6_i386.deb	a775428ebabd852f371a2c3d0b488b16
nessusagent-6.10.4.dmg	7ba1bdcb5c802d6547d7c758828dd2c1
nessusagent-6.10.4-es5.i386.rpm	ee0bcbedd00cbed71cd2e11ebfff1df4
nessusagent-6.10.4-es5.x86_64.rpm	75c19d4a440bab3965534ed942cf0116
nessusagent-6.10.4-es6.i386.rpm	37fc225409b888782ac9e92c848a9ce6
nessusagent-6.10.4-es6.x86_64.rpm	7b1a31636b1a343f375bb8200bc60d25
nessusagent-6.10.4-es7.x86_64.rpm	45339d3dda09e13983cf81258fc23114
nessusagent-6.10.4-fc20.x86_64.rpm	28edb3f4876e87a612315592ca2e6dc9

File	MD5
nessusagent-6.10.4-suse11.i586.rpm	1731b75181b21d796275affde61130f5
nessusagent-6.10.4-suse11.x86_64.rpm	f61c0f1f3eb6639765135a45879f3bb6
nessusagent-6.10.4-suse12.x86_64.rpm	98e811fdbeee53564d867be11613ba7c
nessusagent-6.10.4-ubuntu1110_amd64.deb	52e198ea0c9560cdbaaef80529d0b63f
nessusagent-6.10.4-ubuntu1110_i386.deb	ecd43a9c3c3450c4825328424cf64da4
nessusagent-6.10.4-ubuntu910_amd64.deb	f217fc76355d0bce71a3d678459838f1
nessusagent-6.10.4-ubuntu910_i386.deb	718171b44adbe6ea472e55852cfe1e9b
nessusagent-6.10.4-Win32.msi	8d8429489a4293ce0488801f6eca15d8
nessusagent-6.10.4-x64.msi	2350b620d8170d4b227ef814bde904d0

Nessus Agent 6.10.5 Release Notes - 4/11/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features / Expanded Platform Support

- Enable users to see the status of connected agents
- Enable users to see more details (status, attributes) about agents
- Enable users to manage when agent updates do and don't occur
- Enable users to download updates for agents

Bug Fixes and Improvements

- Fix for a local privilege escalation vulnerability on agent

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.5-amzn.x86_64.rpm	48d562c25d7548e818584cad13a20ad3
nessusagent-6.10.5-debian6_amd64.deb	3bf4666797086133c532f0afe0a5921f

File	MD5
nessusagent-6.10.5-debian6_i386.deb	afa71350d7272880c13d03ef829665ab
nessusagent-6.10.5.dmg	8ce94f120297248f82a329b37ae05566
nessusagent-6.10.5-es5.i386.rpm	673ee9b3717ae759b9b9520609071add
nessusagent-6.10.5-es5.x86_64.rpm	ae0234e38af680ce5cde8a8082b496d3
nessusagent-6.10.5-es6.i386.rpm	c34b600e23dbc63e710204933cafc26a
nessusagent-6.10.5-es6.x86_64.rpm	25afd5f9b670c3d327ef10a0939fbf40
nessusagent-6.10.5-es7.x86_64.rpm	eb33547910fb4f70aadf4f414a753610
nessusagent-6.10.5-fc20.x86_64.rpm	5c1c84641c14af318a955022c3eb39ec
nessusagent-6.10.5-suse11.i586.rpm	bb8023f4f99d64e85d5c2ee36f601478
nessusagent-6.10.5-suse11.x86_64.rpm	60ffdba918eb3cd3d09d2c99843d90ab
nessusagent-6.10.5-suse12.x86_64.rpm	67543a54ac1b30ca0211ff3bdd56fadd
nessusagent-6.10.5-ubuntu1110_amd64.deb	4c72583c85c982ccd714809a8276bc5b
nessusagent-6.10.5-ubuntu1110_i386.deb	69085f304e8dfadfa3f70593cedb79f0
nessusagent-6.10.5-ubuntu910_amd64.deb	57a65cf99f1877de3cfa37aa9a15d05a
nessusagent-6.10.5-ubuntu910_i386.deb	274fc3cadc5e36b029aa99ca4484a3b8
nessusagent-6.10.5-Win32.msi	58e2c1d09354b27b2231ac059d1be118
nessusagent-6.10.5-x64.msi	c1102cff319dfcf683be959942c56d8e

Nessus Agent 6.10.6 Release Notes - 5/24/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes and Improvements

- Allow user-agent field to be edited

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.6-amzn.x86_64.rpm	c6a84765d070a8a355804fec653fd8a7
nessusagent-6.10.6-debian6_amd64.deb	440096986d01280b10fb92e71d35babd
nessusagent-6.10.6-debian6_i386.deb	dbfae4825074da66b991319ae7599217
nessusagent-6.10.6.dmg	13957a4ac33900329737c54acae8e366
nessusagent-6.10.6-es5.i386.rpm	488ef39491bbaf68ea624f3f517dab3b
nessusagent-6.10.6-es5.x86_64.rpm	e77796c4d2709230a7ded90de8598184
nessusagent-6.10.6-es6.i386.rpm	6482cb322373788f30e5a3565d2fafd9
nessusagent-6.10.6-es6.x86_64.rpm	e5e870db2c524d173444599626982a7d
nessusagent-6.10.6-es7.x86_64.rpm	160b629878fe5b5680e62689c7957aa3
nessusagent-6.10.6-fc20.x86_64.rpm	6fb0089e743c38f01902564d289eb0c2
nessusagent-6.10.6-suse11.i586.rpm	1322da6cc0b0ed86b20ee6976afece69
nessusagent-6.10.6-suse11.x86_64.rpm	6a0ffe212439da9fec1da425fba6103b
nessusagent-6.10.6-suse12.x86_64.rpm	241c6d94f9813ba6f2aacdebe9e2dfa3
nessusagent-6.10.6-ubuntu1110_amd64.deb	10137a2fc9465ae1fe17b3ce48981ff5
nessusagent-6.10.6-ubuntu1110_i386.deb	e0bc2ef8a6391c027999621177a35be8
nessusagent-6.10.6-ubuntu910_amd64.deb	8ccc43fd857289b4f3cb0f3e6f6dbbad
nessusagent-6.10.6-ubuntu910_i386.deb	88cc37b7d5c9657faf191da0a9a0a6fd
nessusagent-6.10.6-Win32.msi	a4864e28cdb3229dd22c4e8aeca011f3
nessusagent-6.10.6-x64.msi	cbfecff75ab9a82db62721f09167e1a0

Nessus Agent 6.10.7 Release Notes - 5/31/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.7-amzn.x86_64.rpm	350c1b60d2ccc75dc867e7725d5b41ac
nessusagent-6.10.7-debian6_amd64.deb	7bac430cc411e241197c5031fa775cb8
nessusagent-6.10.7-debian6_i386.deb	98e52deab2c92608bd3e6b6e5dd64844
nessusagent-6.10.7.dmg	6e46d6b315d19d9f26964003ec319e0d
nessusagent-6.10.7-es5.i386.rpm	5be01c1da4bda3fbe46b33747c3c56ef
nessusagent-6.10.7-es5.x86_64.rpm	ec4ebba5d224f0ca51868bafeb590ab9
nessusagent-6.10.7-es6.i386.rpm	667a8ffdd3811a9ee18c42c61179ebea
nessusagent-6.10.7-es6.x86_64.rpm	cd40892e9c7e4543ba1c5b487a9da220
nessusagent-6.10.7-es7.x86_64.rpm	0ffec709084e91c5edc82480497841e3
nessusagent-6.10.7-fc20.x86_64.rpm	e4bdb71ccf6322d07a140128c9e6d448
nessusagent-6.10.7-suse11.i586.rpm	39fa63f40585ac9c6a4cc5bd49c10416
nessusagent-6.10.7-suse11.x86_64.rpm	a32642780c3cfdcd4786b95711b392d2
nessusagent-6.10.7-suse12.x86_64.rpm	a5e7e2fb155316db56bfe1fd84fe658d
nessusagent-6.10.7-ubuntu1110_amd64.deb	6784fb3ef79a98199285816972bf62e5
nessusagent-6.10.7-ubuntu1110_i386.deb	4074d5b209291b67d10dfd70acb994ab
nessusagent-6.10.7-ubuntu910_amd64.deb	0be545a957e274b8e129bfe5e5144960
nessusagent-6.10.7-ubuntu910_i386.deb	deea1711e57ced82fa41fc089e335b2b
nessusagent-6.10.7-Win32.msi	94683c259c9cae34de999007f8f1ec33
nessusagent-6.10.7-x64.msi	797c71afd810073ac4df374fabc96711

Nessus Agent 6.10.8 Release Notes - 6/21/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.8-amzn.x86_64.rpm	ec8628cc90a97ce9f061d4892db583e1
nessusagent-6.10.8-debian6_amd64.deb	674f39b3f25dd2752d9955380021cb8f
nessusagent-6.10.8-debian6_i386.deb	ab5068b9a26a7096b025c4344bb3c515
nessusagent-6.10.8-es5.x86_64.rpm	e89e4ea0d6163c5c9dd44b5d81a88203
nessusagent-6.10.8-es5.i386.rpm	63a2ec12b66c5c72164a5892189a9dd2
nessusagent-6.10.8-es6.x86_64.rpm	3d2d9ecb2b1906355646917e9c1063dd
nessusagent-6.10.8-es6.i386.rpm	7c122b1ee15aee95d745b68fe0214707
nessusagent-6.10.8-es7.x86_64.rpm	7d3ee804e4813beaea8ee916c7c82e46
nessusagent-6.10.8-fc20.x86_64.rpm	e75ec3a03d071baee23d43080be252f5
nessusagent-6.10.8.dmg	50b5d34202d47fa85abe6d907cb74807
nessusagent-6.10.8-suse11.x86_64.rpm	60d9f8a0390b44904da1a281180e688f
nessusagent-6.10.8-suse11.i586.rpm	1d09a906d8e67ca24d23d1d57b1354ed
nessusagent-6.10.8-suse12.x86_64.rpm	0bd3c944db18ac579ceb72a266839b1d
nessusagent-6.10.8-ubuntu1110_amd64.deb	ab3a6d19a4e97e672bdce51cb874f697
nessusagent-6.10.8-ubuntu1110_i386.deb	f720b1c367b8adf775d7d2099bf53966
nessusagent-6.10.8-ubuntu910_amd64.deb	52744cf4c9659aa180d6ff96deabc4d4
nessusagent-6.10.8-ubuntu910_i386.deb	df519006349768f4a44e6913e200bc59
nessusagent-6.10.8-Win32.msi	c44e0b82610c62e622e7bc877a235573
nessusagent-6.10.8-x64.msi	0d4f37852fd278358292a69d39627471

Nessus Agent 6.10.9 Release Notes - 7/14/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

File Names & MD5 Checksums

File	MD5
nessusagent-6.10.9-amzn.x86_64.rpm	4f4d86abedaa5017f72e339d43d1102d
nessusagent-6.10.9-debian6_amd64.deb	f0497bbb89979bb779b3dbd7ed4dd193
nessusagent-6.10.9-debian6_i386.deb	a888e7d4d32a917f360244fc6e031385
nessusagent-6.10.9.dmg	1ce564f6dfaa878963b0fc1551ad6bad
nessusagent-6.10.9-es5.i386.rpm	769cc48c1d01e96fadff9e4978372b36
nessusagent-6.10.9-es5.x86_64.rpm	7d9990e5c6454256c1b272acbec7e63f
nessusagent-6.10.9-es6.i386.rpm	967307cce60fbc7b3064ff360e56ac88
nessusagent-6.10.9-es6.x86_64.rpm	c2452077cfc57a95ba89437c809b82e4
nessusagent-6.10.9-es7.x86_64.rpm	a05da90ed88e6eaa4d67db144dfa2009
nessusagent-6.10.9-fc20.x86_64.rpm	70328eebe02c5fca33d5f69456abf471
nessusagent-6.10.9-suse11.i586.rpm	ff01840d6b7b03f3d4388bd128d3c7e4
nessusagent-6.10.9-suse11.x86_64.rpm	ad50e21cf77c6cf1f58e83a4620a770d
nessusagent-6.10.9-suse12.x86_64.rpm	7a8492bb7e2b5bf4414ff541cbe92b0f
nessusagent-6.10.9-ubuntu1110_amd64.deb	fbdff960ab6ab75a8ef1f3226109babc
nessusagent-6.10.9-ubuntu1110_i386.deb	81a5d3e38f18ee315e6cb9ee9b772d04
nessusagent-6.10.9-ubuntu910_amd64.deb	98fef19a5b61639289cba06492be3526
nessusagent-6.10.9-ubuntu910_i386.deb	d204bf38d9be5894fc08e5a9aafdf9f1
nessusagent-6.10.9-Win32.msi	964408138ddfacb6a9b1c507b62133ea
nessusagent-6.10.9-x64.msi	4b2fb90f9709b1a39e2e0dc2dabeb84d

Nessus Agent 6.11.0 Release Notes - 8/7/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features/Expanded Platform Support

- Add multiple agents to a group at once
- Automatically unlink agents after a period of inactivity

File Names & MD5 Checksums

File	MD5
nessusagent-6.11.0-amzn.x86_64.rpm	5ed4ebc5256f8fca11d59f5a49acad2c
nessusagent-6.11.0-debian6_amd64.deb	fcd57ff51f1c0bedfa489527e34b759f
nessusagent-6.11.0-debian6_i386.deb	d4313e4d685201e192173f024044a8af
nessusagent-6.11.0.dmg	4194206e0e2a634c67066914b9a3102b
nessusagent-6.11.0-es5.i386.rpm	7d9a7745264002039780b9513f087d92
nessusagent-6.11.0-es5.x86_64.rpm	2466397c8348b9f2c7defc5cf774b620
nessusagent-6.11.0-es6.i386.rpm	09f243650e8841559273d119dcec4028
nessusagent-6.11.0-es6.x86_64.rpm	0d522b6f23c37a0dbbd78cfd4c855d71
nessusagent-6.11.0-es7.x86_64.rpm	aa17609e955fb4b5195a64ce093b6fb3
nessusagent-6.11.0-fc20.x86_64.rpm	12f1165799c82e984ce6d8059286777b
nessusagent-6.11.0-suse11.i586.rpm	d083d141ecf3604b4bfaea39bcc0544e
nessusagent-6.11.0-suse11.x86_64.rpm	f225d7e404b8abf755ae3127a564ffd7

File	MD5
nessusagent-6.11.0-suse12.x86_64.rpm	4625562c72e6e69c8ada305d0c1a1d33
nessusagent-6.11.0-ubuntu1110_amd64.deb	b2f8d489bf364ad6158b6318cf178013
nessusagent-6.11.0-ubuntu1110_i386.deb	00b0901d7e0cada6762ce5007c4a1b0d
nessusagent-6.11.0-ubuntu910_amd64.deb	75c805d90548984a56232e3e97c0ac54
nessusagent-6.11.0-ubuntu910_i386.deb	3fc31ccf5ffd383e275dc248706f106
nessusagent-6.11.0-Win32.msi	f021a354c8bdbf36e1c5f6579af31e95
nessusagent-6.11.0-x64.msi	5bec76958ddfb8e26063efe470510456
nessus-updates-6.11.0.tar.gz	e26d24e5920f9367e9af7ea312e1069b

Nessus Agent 6.11.1 Release Notes - 8/14/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

File Names & MD5 Checksums

File	MD5
NessusAgent-6.11.1-es5.x86_64.rpm	6c80764fb922800f99a07b992f1c1394
NessusAgent-6.11.1-es5.i386.rpm	5bf57be05543c2afee490d1ec9dbcba1

File	MD5
NessusAgent-6.11.1-es6.x86_64.rpm	ce16cb2eb66ab5546a8d8bb89231fd2a
NessusAgent-6.11.1-es6.i386.rpm	8b1e2ff08b845353c0242b676cf2de38
NessusAgent-6.11.1-es7.x86_64.rpm	bfbbfbcf6f9204711ab01cd17d328e17
NessusAgent-6.11.1-fc20.x86_64.rpm	bdd4efea8c8cf7a621be15b4a2e92b2d
NessusAgent-6.11.1.dmg	ddec71833f127d4a5be8350fa01f7a76
NessusAgent-6.11.1-suse11.x86_64.rpm	629ef898bf8cf49706a48938e503e3f4
NessusAgent-6.11.1-suse11.i586.rpm	f6466c9acb8d0bd7ce9f4a72705f256f
NessusAgent-6.11.1-suse12.x86_64.rpm	7de30047bdbffa88266d4e097e9191cb
NessusAgent-6.11.1-ubuntu1110_amd64.deb	f71d34599cac4ce657bc4c47a5b583c2
NessusAgent-6.11.1-ubuntu1110_i386.deb	0b51f3fcf31ba7e04962608060c61cea
NessusAgent-6.11.1-ubuntu910_amd64.deb	b35795c3086fecb18d8bb61c898e3e0b
NessusAgent-6.11.1-ubuntu910_i386.deb	61f931b7b96d97754548464000 3883f5
NessusAgent-6.11.1-Win32.msi	c073a38637a46ce1ccbab2576ee1f47c
NessusAgent-6.11.1-x64.msi	7fdfe41cec26cc5db994b4bb11e3566a
nessus-updates-6.11.1.tar.gz	371aef3d2c61c169ce2c37397c7a1e65

Nessus Agent 6.11.2 Release Notes - 10/26/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

File Names & MD5 Checksums

File	MD5
NessusAgent-6.11.2-amzn.x86_64.rpm	d7601087c2ad8286cdffdbff55d9032e
NessusAgent-6.11.2-debian6_amd64.deb	d769e713c307c5264eff25541e097737

File	MD5
NessusAgent-6.11.2-debian6_i386.deb	58bce5c1f8b177659806a25c46fac672
NessusAgent-6.11.2-es5.x86_64.rpm	b7ad5bb3911229c3ff6ca09738283855
NessusAgent-6.11.2-es5.i386.rpm	5f0ade7cdbc877e76a6195064e41a890
NessusAgent-6.11.2-es6.x86_64.rpm	8f987543484206bd653549a497e5a414
NessusAgent-6.11.2-es6.i386.rpm	660478368c5553544ff6c990338fd8a2
NessusAgent-6.11.2-es7.x86_64.rpm	956c220467011548b2a0800c4aa2299e
NessusAgent-6.11.2-fc20.x86_64.rpm	0bbb1d2c96cd85161333ab57cb309222
NessusAgent-6.11.2.dmg	7ca45e2861f71fb54a8b9ccf2a4f6db0
NessusAgent-6.11.2-suse11.x86_64.rpm	0e8e4d019a557e1050a93bfdcc0d6e60
NessusAgent-6.11.2-suse11.i586.rpm	a67ee214ac52bc118b84b8bc2a81d10b
NessusAgent-6.11.2-suse12.x86_64.rpm	ceb4b692f44b8710de981e8ada360fc2
NessusAgent-6.11.2-ubuntu1110_amd64.deb	dc1fb093506c992a961c1c19bbdb61b0
NessusAgent-6.11.2-ubuntu1110_i386.deb	d93e2198f70c42a813ed7c8cad3ac9cb
NessusAgent-6.11.2-ubuntu910_amd64.deb	f4c367bc1414a6cfdbb478a2e4ea7390
NessusAgent-6.11.2-ubuntu910_i386.deb	207e73ec3644eabf175d65fd03ae0eba
NessusAgent-6.11.2-Win32.msi	75a4492653bc744be12fcc8f47154481
NessusAgent-6.11.2-x64.msi	2ddae89d1985c814791e7c47a7c4294f

Nessus Agent 6.11.3 Release Notes - 12/5/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

File Names & MD5 Checksums

File	MD5
NessusAgent-6.11.3-amzn.x86_64.rpm	eca13b982cc3a42c37df4b5976266764
NessusAgent-6.11.3-debian6_amd64.deb	7eeec5a92ddf6b85ef1fb68dd843f430
NessusAgent-6.11.3-debian6_i386.deb	69b23c7570fc4b90dd629f47e6f6ef3f
NessusAgent-6.11.3-es5.x86_64.rpm	9e8e549687ac44c17e764ac1a9846fdb
NessusAgent-6.11.3-es5.i386.rpm	7e790a7c97143965ce0c81d56928acbe
NessusAgent-6.11.3-es6.x86_64.rpm	845fcffd1bfd008654d117d064f29cce
NessusAgent-6.11.3-es6.i386.rpm	31c4b4979e3f09d7518c6d7b4fcd0e9b
NessusAgent-6.11.3-es7.x86_64.rpm	1bcc7214d6971be179eec0928d41cc3c
NessusAgent-6.11.3-fc20.x86_64.rpm	322863807e0ea4ff2699a82f66ba4889
NessusAgent-6.11.3.dmg	9384c88ba72e0943fed53a46798fe3e2
NessusAgent-6.11.3-suse11.x86_64.rpm	49ae264a07197b568791df86bd434d1d
NessusAgent-6.11.3-suse11.i586.rpm	db9ba5dba8bda153e76c058e47be0efd
NessusAgent-6.11.3-suse12.x86_64.rpm	c8508669510d1b4e6f2570781ed92d9d
NessusAgent-6.11.3-ubuntu1110_amd64.deb	f6c3bd8a2fc7aaf577a5f1f5f10bcf0c
NessusAgent-6.11.3-ubuntu1110_i386.deb	00a85553d0f75316c1de180e1854cd6a
NessusAgent-6.11.3-ubuntu910_amd64.deb	7945eec9f5d302dc852be0df3111de05
NessusAgent-6.11.3-ubuntu910_i386.deb	0206c6f7d64a41dc002ac8ab1b63b95b
NessusAgent-6.11.3-Win32.msi	8a086bb1421b06dfeec0a61980172f11
NessusAgent-6.11.3-x64.msi	cbe4292e43c0e33009a99b5f5d59f79b

Nessus Agent 7.0.0 Release Notes - 12/12/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus Agent, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes

- Typo in Agent backend.log

File Names & MD5 Checksums

File	MD5
NessusAgent-7.0.0-amzn.x86_64.rpm	c8cc067b21925fe7f435b79276199ed4
NessusAgent-7.0.0-debian6_amd64.deb	48d426900392dee9e107e56ed78f9c40
NessusAgent-7.0.0-debian6_i386.deb	37445ece0f6cbc57ed4150630ef8d836
NessusAgent-7.0.0-es5.x86_64.rpm	af9ec38ed8e9a0ae37af7aa21a38e09c
NessusAgent-7.0.0-es5.i386.rpm	6d143848f4f4748722261e27232328fb
NessusAgent-7.0.0-es6.x86_64.rpm	47b14b32086a8acb4b25c09ad3f801b1
NessusAgent-7.0.0-es6.i386.rpm	cd5f1f52a80cc383f96d858c205a0769
NessusAgent-7.0.0-es7.x86_64.rpm	4f1e9bb8963e2530f338014df5bda9de
NessusAgent-7.0.0-fc20.x86_64.rpm	b9a8456147fa4ecf1935b536453b4a42
NessusAgent-7.0.0.dmg	825afa3c82ec4790f75029e8f2a94c01
NessusAgent-7.0.0-suse11.x86_64.rpm	7ea534e85cadeeeabb755136674638e9
NessusAgent-7.0.0-suse11.i586.rpm	53aec1d4d0b9917933a18e453348b9b1
NessusAgent-7.0.0-suse12.x86_64.rpm	6f68476136bd7b42c2c4ca33b0fdfd04
NessusAgent-7.0.0-ubuntu1110_amd64.deb	050b98d68843d984872de7a9c6d3a87c
NessusAgent-7.0.0-ubuntu1110_i386.deb	d8b456473f0e8821797277c4446125df
NessusAgent-7.0.0-ubuntu910_amd64.deb	1d5cf07078e1943f3a6ebbed7863415e
NessusAgent-7.0.0-ubuntu910_i386.deb	bc5ee800c7ed54efd8f4ab4a7167f24b

File	MD5
NessusAgent-7.0.0-Win32.msi	e57633b478f3ebbbd91d5bf158aef684
NessusAgent-7.0.0-x64.msi	a4b6895f799853b99c0e4c662cf35eca

Tenable Network Monitor Release Notes

To view EOL Tenable Network Monitor release notes, see Tenable EOL Release Notes.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

View the following Tenable Network Monitor (formerly NNM) release notes:

2022 Tenable Network Monitor

Nessus Network Monitor 6.1.1 - Release Notes - 2022-11-08

> **Note:** Standard support for Tenable Network Monitor 5.12 ended on 09/30/2022. Tenable recommends updating to Tenable Network Monitor 5.13.1 or later. Otherwise, you will not be able to report issues and

ugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to enable Network Monitor 6.1.1.

Changed Functionality and Performance Enhancements

Tenable Network Monitor 6.1.1 includes a patch for OpenSSL 3.0.5 to upgrade to OpenSSL 3.0.7.

Supported Platforms

Support is available for the following platforms:

- Red Hat 7 / CentOS 7, version 7.9 (64-bit)
- Red Hat 8 / CentOS 8, versions 8.2-8.5 (64-bit)
- Microsoft Windows 10 and Windows Server 2012/2016 (all 64-bit)

Nessus Network Monitor 6.1.0 - Release Notes - 2022-09-20

> **Note:** Standard support for Tenable Network Monitor 5.12 ended on 09/30/2022. Tenable recommends updating to Tenable Network Monitor 5.13.1 or later. Otherwise, you will not be able to report issues and bugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to Tenable Network Monitor 6.1.1.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Network Monitor 6.1.0:

- Support OpenSSL 3.0:
  - Tenable Network Monitor 6.1.0 includes security enhancements to support OpenSSL 3.0. The default connection mode of Tenable Network Monitor 6.1.0 is TLS 1.2.
- Support for cloud.tenable.com's new Web Application Firewall (WAF):
  - Supports enhanced security for Tenable Vulnerability Management connections.
- User interface Security Enhancements.
- Update Tenable Network Monitor's Key to use SHA-2 signing instead of SHA-1.

- Enhance Tenable Network Monitor to send vulnerabilities for the last hour when connecting to Tenable Vulnerability Management for the first time.

For more information about the features and functionality supported in this release, see the Nessus Network Monitor 6.1.x User Guide and the Nessus Network Monitor Deployment Guide.

Release Notes

The following are updates included in Tenable Network Monitor 6.1.0:

- Tenable Network Monitor's rpm's are now signed with a 4096 bit signature using SHA256.
- If you are running Tenable Network Monitor in NIAP mode using the default Tenable Network Monitor self-signed certificates or if your CA signed certificates are missing the Authority Key Identifier or Subject Key Identifier, OpenSSL 3.0 considers your SSL certificates to be invalid. Tenable Network Monitor disables NIAP Mode for these conditions and issue a message in the UI when the user logs on.
- The latest patches from js.node are included as part of this release.
- If you connect to Tenable Vulnerability Management using a Web Proxy, you must upgrade to Tenable Network Monitor 6.1.0.

Supported Platforms

Support is available for the following platforms:

- RH7/CentOS7, version 7.9 (64-bit)
- RH8/CentOS8, versions 8.2-8.5 (64-bit)
- Microsoft Windows 10 and Windows Server 2012/2016 (all 64-bit)

Nessus Network Monitor 6.0.1 - Release Notes - 2022-05-09

> **Note:** Standard support for Tenable Network Monitor 5.12 ended on 09/30/2022. Tenable recommends updating to Tenable Network Monitor 5.13.1 or later. Otherwise, you will not be able to report issues and bugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to Tenable Network Monitor 6.1.1.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Network Monitor 6.0.1:

- **Enhanced Trending Charts:**
    - Trending charts and SIEM events can now show trends in days and weeks depending on the sample time defined by the user. Users can change the default sample time of one minute up to an hour, extending the time to weeks to spot long-term trends.
- **SIEM Analysis for Tenable Network Monitor Snapshots:**
    - Users can now drill down exclusively on SIEM events when viewing Tenable Network Monitor snapshots.
- **Enhanced Security for SIEM Integration:**
    - The passwords used to connect to an external SIEM solution are now encrypted in the Nessus Network Monitor Database, keeping them secret to users.

For more information about the features and functionality supported in this release, see the Nessus Network Monitor 6.0.x User Guide and the Nessus Network Monitor Deployment Guide.

Security Updates

The following are security updates included in Tenable Network Monitor 6.0.1:

- Upgrade Tenable Network Monitor to openssl 1.1.1n
- Encrypt passwords to SIEM servers
- jQuery UI 1.13.0 Multiple Vulnerabilities (XSS) - NNM
- NNM6 has insecure RPATH

  .

Supported Platforms

Support is available for the following platforms:

- RH7/CentOS7, version 7.9 (64-bit)
- RH8/CentOS8, versions 8.2-8.5 (64-bit)

- MacOS 10.9-10.13 (64-bit)

- Microsoft Windows 7/8/10 and Windows Server 2008/2012/2016 (64-bit)

> **Note:** This is the final release with support for Microsoft Windows 7/8 and Windows Server 2008.

Nessus Network Monitor 6.0.0 - Release Notes - 2022-01-05

> **Note:** Standard support for Tenable Network Monitor 5.12 ended on 09/30/2022. Tenable recommends updating to Tenable Network Monitor 5.13.1 or later. Otherwise, you will not be able to report issues and bugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to Tenable Network Monitor 6.1.1.

New Features

The following are the new features included in Tenable Network Monitor 6.0.0:

- **SIEM Analysis** - Added the ability to connect to Splunk (SIEM) and collect logs through pre-defined queries at regular intervals to identify risk-altering events.

  > **Note:** The SIEM servers functionality is available only for ES/CentOS 7 and 8 platforms (for more information, see the *SIEM Servers* section of Tenable Network Monitor Settings Section). To enable the new processing of SIEM servers, such as Splunk, you must deploy Tenable Network Monitor 6.0.0 using the RPMs for ES/CentOS 7 and 8.

  > **Note:** You need to manually uninstall and reinstall Tenable Network Monitor from its RPM to use the **SIEM Analysis** feature (for example, `rpm -U nnm-6.0.0-es7.x86_64.rpm`, or `rpm -i nnm-6.0.0-es8.x86_64.rpm` for a new deployment).

- Added support for RH8/CentOS8 (8.4 and 8.5).

For more information about the features and functionality supported in this release, see the Nessus Network Monitor 6.0.x User Guide and the Nessus Network Monitor Deployment Guide.

Changed Functionality and Performance Enhancements

The following are changed functionality and performance enhancements included in Tenable Network Monitor 6.0.0:

- **Disable CBC Ciphers Option** - Added the ability to disable CBC ciphers in the Configuration Web Server settings.

Security Updates

The following are security updates included in Tenable Network Monitor 6.0.0:

- Updated OpenSSL to the latest version, 1.1.1l.

Supported Platforms

Support is available for the following platforms:

- RH8/CentOS7, version 7.9 (64-bit)
- RH8/CentOS8, versions 8.2-8.5 (64-bit)
- MacOS 10.9-10.13 (64-bit)
- Microsoft Windows 7/8/10 and Windows Server 2008/2012/2016 (64-bit)

2021 Tenable Network Monitor

Nessus Network Monitor 5.13.0 Release Notes - 2021-02-17

Nessus Network Monitor 5.13.1 Release Notes - 2021-05-11

Nessus Network Monitor 5.13.0 Release Notes - 2021-02-17

> **Note:** Standard support for Tenable Network Monitor 5.12 ended on 09/30/2022. Tenable recommends updating to Tenable Network Monitor 5.13.1 or later. Otherwise, you will not be able to report issues and bugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to Tenable Network Monitor 6.1.1.

New Features

The following are the new features included in Tenable Network Monitor 5.13:

- Added support for Windows Server 2019
- Added support for Red Hat Enterprise Linux/CentOS 7.9
- Added support for Red Hat Enterprise Linux 8.0/CentOS 8.0.

Changed Functionality and Performance Enhancements

The following are other updates included in Tenable Network Monitor 5.13 as security enhancements:

- Updated Tenable Network Monitor to use jQuery v3.5.1 and other UI upgrades, to address a vendor-reported cross-site scripting vulnerability. For more information, see the Tenable Product Security Advisory.
- Updated Tenable Network Monitor to use the latest Microsoft Universal C Runtime Redistributable to get the latest security fixes from Microsoft.

  > **Note:** Tenable Network Monitor requires Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. Existing users connected to the Tenable feed will get the required files automatically.
  >
  > For users on older Windows installations or using the `nnm-5.13.0-x64.exe` package for a fresh installation or upgrade, ensure that you download the specific package `vc_redist.x64.exe` from the Microsoft downloads site.

Bug Fixes

Bug Fix	Defect ID
Addressed an issue where the email settings did not allow the use of the # character.	01115122
Support vxlan traffic decoding to fix problem where Tenable Network Monitor was not able to detect Version of Firefox & HTTP service (AWS VPC traffic mirroring)	01104141

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 6 / CentOS 6 - 64-bit
- Red Hat Linux ES 7 / CentOS 7 - 64-bit (includes support for RH/CentOS Version 7.9 through kernel version 3.10.10-1160)
- Red Hat Linux ES 8/ CentOS 8 - 64 Bit

- MacOS 10.9 - 10.13 - 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 - all 64-bit

Nessus Network Monitor 5.13.1 Release Notes - 2021-05-11

> **Note:** Standard support for Tenable Network Monitor 5.12 ended on 09/30/2022. Tenable recommends updating to Tenable Network Monitor 5.13.1 or later. Otherwise, you will not be able to report issues and bugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to Tenable Network Monitor 6.1.1.

New Features

The following are the new features included in Tenable Network Monitor 5.13.1:

- **Tenable Network Monitor Proxy Support for Tenable Vulnerability Management** - Customers can now connect Tenable Network Monitor to Tenable Vulnerability Management using their company's web proxy. For more information, see Web Proxy Settings in the *Tenable Network Monitor User Guide*.
- Added support for Red Hat Enterprise Linux / CentOS 8.3.

For more information about the features and functionality supported in this release, see the Nessus Network Monitor 5.13.x User Guide.

Security Updates

The following are security updates included in Tenable Network Monitor 5.13.1:

- Updated OpenSSL to the latest version, 1.1.1k. For more information, see the Tenable Product Security Advisory.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where Tenable Network Monitor showed a false error when user would set the "Monitored Network IP Addresses and Ranges" from the command line.	01178101

Upgrade Considerations

If you deployed Tenable Network Monitor 5.13.0 on Red Hat/CentOS 8, you must upgrade to Tenable Network Monitor 5.13.1 using the RPM software package from the Tenable Downloads site.

To deploy the RPM:

```
rpm -U nnm-5.13.1-es8.x86_64.rpm
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 6 / CentOS 6 - 64-bit
- Red Hat Linux ES 7 / CentOS 7 - 64-bit (includes support for RH/CentOS Version 7.9 through kernel version 3.10.10-1160)
- Red Hat Linux ES 8/ CentOS 8 - 64 Bit
- MacOS 10.9 - 10.13 - 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016/2019 - all 64-bit

2020 Tenable Network Monitor

Nessus Network Monitor 5.11.1 Release Notes - 2020-06-02

Nessus Network Monitor 5.12.0 Release Notes - 2020-09-29

Nessus Network Monitor 5.12.1 Release Notes - 2020-11-05

Nessus Network Monitor 5.11.1 Release Notes - 2020-06-02

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changed Functionality and Performance Enhancements

The following updates were added in Tenable Network Monitor 5.11.1:

- Upgraded to OpenSSL 1.1.1g
- Upgrade to DPDK-19.11.2

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.8)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Nessus Network Monitor 5.12.0 Release Notes - 2020-09-29

Changed Functionality and Performance Enhancements

The following updates were added in Tenable Network Monitor 5.12.0:

- Finalized work to provide FIPS compliant SSL communications.
- Certificate handling enhancements to support future certification efforts.

Bug Fixes

Bug Fix	Defect ID
Resolved issue where Tenable Network Monitor configuration would reset after rebooting on a Tenable Core image	01036646
Addressed issue where Tenable Network Monitor would hang after attempting an export of HTML Summary Reports	00945620

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit

- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.7 through kernel version: 3.10.0-1062)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Nessus Network Monitor 5.12.1 Release Notes - 2020-11-05

Bug Fixes

Note: This release includes a fix for a potential vulnerability. For more information see the Tenable Product Security Advisory.

Bug Fix	Defect ID
Addressed issue where Nessus Network Monitor would show as online within Tenable Vulnerability Management, but would not show a valid Plugin set even though one was present.	01089020

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.7 through kernel version: 3.10.0-1062)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

2019 Tenable Network Monitor

2019 Tenable Network Monitor

Nessus Network Monitor 5.10.0 Release Notes - 2019-09-05

Nessus Network Monitor 5.10.1 Release Notes - 2019-10-08

Nessus Network Monitor 5.11.0 Release Notes - 2019-12-18

Nessus Network Monitor 5.8.0 Release Notes - 3/5/2019

Nessus Network Monitor 5.8.1 Release Notes - 2019-03-28

Nessus Network Monitor 5.9.0 Release Notes - 2019-06-03

Nessus Network Monitor 5.9.1 Release Notes - 2019-07-25

2019 Tenable Network Monitor

Nessus Network Monitor 5.10.0 Release Notes - 2019-09-05

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

The following new features were added in Tenable Network Monitor 5.10.0:

- Upgraded OpenSSL library to version openssl-1.0.2.s
- Support for Napatech Acceleration Cards: NT40E3-4-PTP
  - Available for users using this version of the Napatech drivers.
- Support Strong Encryption Ciphers for TLS v1.2

  If enabled, the following ciphers are used:

  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384

    - TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
    - TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

  If disabled, the following ciphers are used:

    - TLS_RSA_WITH_AES_128_CBC_SHA
    - TLS_RSA_WITH_AES_256_CBC_SHA

The following feature does not require a license, and will not count against the license asset count for Tenable Vulnerability Management or Tenable Security Center:

- Asset Discovery Mode - Intended for basic asset discovery via reporting of the following detections for an asset:
    - Open Port
    - Number of Hops
    - Generic Protocol Detection
    - VLAN ID Detection
    - Generic IPv6 Tunnel Traffic Detection
    - VXLAN ID Detection
    - Host Attribute Enumeration

The following feature is only available as premium content for Tenable Network Monitor users with a paid subscription to Industrial Security:

- Support for the following protocols:
    - Hart IP
    - VNet/IP v2 Protocol
    - Saia Burgess EtherSBus Protocol
    - OMRON/FINS Support for Non-Standard Ports.
    - Discovery of 130+ Protocols by Port Detections List.
    - Honeywell FTE Protocol version parsing.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.6 through kernel version: 3.10.0)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Nessus Network Monitor 5.10.1 Release Notes - 2019-10-08

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

Note: These new features are only available with an Industrial Security subscription and are available only when Tenable Network Monitor is connected to Industrial Security.

The following are new features included in Tenable Network Monitor 5.10.1:

- Support for the following protocols:
  - DNP3 over UDP
  - Mitsubishi MelsecModbus over UDP
  - CIP/PCCC
  - Cisco Discovery Protocol (CDP)
  - Modbus RTUCIP-CM
- In addition to the above, the following protocols were extended to enhance detection performance:
  - Additional CIP attributes from 'Get Attr All' messages
  - Additional devices from SNMP OID information.

- An OT Derivative Detection was added to allow Industrial Security to pass System Types to Tenable Security Center and Tenable Vulnerability Management via it's own plugin

All Tenable Network Monitor customers will enjoy the following new features:

- Expanded RH/CentOS 7 support to include Version 7.7 through kernel version 3.10.0-1062.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.6 through kernel version: 3.10.0-1062)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Nessus Network Monitor 5.11.0 Release Notes - 2019-12-18

New Features

The following new features were added in Tenable Network Monitor 5.11.0.

NIAP Improvements

- TLS Client Protocol verification of identifiers per RFC 6125
- IS Application shall not establish connection if the peer certificate is invalid
- Integration of OpenSSL 1.1.1d

VRB Improvements

- Redirect HTTP to HTTPS. CVE: N/A
- jquery.js, moment.js version upgrades to fix vulnerabilities. CVE: N/A
- Miscellaneous HTTP Header additions: Content Security Policy, Cache Control, Pragma. CVE:

N/A

- Installshield Upgrade to prevent use of malicious dll's. CVE-2016-2542

Support for the following protocols:

> **Note:** The following features added in Tenable Network Monitor 5.11.0 are only available as premium content for Tenable Network Monitor users with a paid subscription to Industrial Security.

- Improvement to SBC protocol dissection to perform asset and vuln lookup.
- Improvement to BACnet protocol dissection to perform asset and vuln lookup.
- Improvement to DeltaV protocol dissection to perform asset and vuln lookup.
- Method for extracting asset information from text-based protocols (new plugin keywords).
- ECOM protocol support
- Beckhoff AMS/ADS protocol support

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.7 through kernel version: 3.10.0-1062)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Nessus Network Monitor 5.8.0 Release Notes - 3/5/2019

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features and Changed Functionality

> **Note:** These features are only available with an Industrial Security subscription.

The following are new OT-related features included in Tenable Network Monitor 5.8.0:

- Addition of over 4,000 new ICS asset detections that include:
  - 3,467 new Yokogawa devices
  - 468 new Schneider Electric devices
  - 58 new Emerson devices
  - 17 new Siemens devices
  - 7 new GE devices
  - 4 new ABB devices
  - 2 new Mitsubishi devices
- Expansion of OT vulnerability detections - more than tripled industrial device-related vulnerability coverage to over 220 CVEs.
- The following new ICS protocols are now supported:
  - Omron-FINS
  - Yokogawa RPS

In addition, all Tenable Network Monitor customers will enjoy:

- Expansion of mobile device and O/S detections to include recent iPhone and iOS versions
- Support for the most recent RH/CentOS 7.6 Kernel Versions (see Supported Platforms below)

Changed Functionality

The following functionality has been changed in Tenable Network Monitor 5.8.0 GA:

- PII Obfuscation is now enabled by default. For versions of Tenable Network Monitor connected to other applications (SecurityCenter, SCCV, Tenable Vulnerability Management and Industrial Security), this feature, which masks PII when enabled, cannot be disabled. For stand alone instances of Tenable Network Monitor, this feature can be disabled from the Configuration → General Tab → Advanced drop-down option by the same name (simply change 1 to 0 and click the Save button).

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (NEW! Support for RH/CentOS Version 7.6 through kernel version: 3.10.0-957)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Be Advised:

- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.4.1 are supported. Installations running previous versions of Tenable Network Monitor 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to Tenable Network Monitor 5.8.0 - Refer to the Tenable Network Monitor 5.8.0 User Guide for details on upgrading to Tenable Network Monitor 5.8.0.
- Tenable Network Monitor 5.8.0 is compatible with SecurityCenter 4.7.x and later.
- Tenable Network Monitor 5.8.0 is compatible with Industrial Security 1.3.1 and later.
- The Tenable Network Monitor Web Server and Tenable Network Monitor HTML5 User Interface are each automatically updated to version 2.4.0 via a plugin update.

Nessus Network Monitor 5.8.1 Release Notes - 2019-03-28

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

> **Note:** These new features are only available with an Industrial Security subscription and are available only when Tenable Network Monitor is connected to Industrial Security.

The following are new OT-related features included in Tenable Network Monitor 5.8.1:

- Expansion of ICS asset detections to include:
    - 358 newly supported Emerson/DeltaV Devices
    - 91 newly supported Siemens Devices
- Expansion of OT vulnerability detections to include:
    - 77 newly supported ICS-specific vulnerability detections
- Expanded OT protocol detections to include:
    - Full parsing, protocol detection and device detection for Emerson ROC and Yokogawa HLLS Protocol.
- Port-based Protocol Detection for:
    - Emerson DeltaV Protocol (UDP Port 18507)
    - Emerson ROC Protocol (TCP Port 4000)
    - Moxa Protocol (TCP Port 4502, UDP Port 4800, TCP Port 4900)
    - Omron FINS Protocol (TCP Port 9600, UDP Prot 9600)
    - RedLion Crimson Protocol (TCP Port 789)
    - Rockwell PCCC/CSP (TCP Port 2222)
    - Schneider TriStation Protocol (UDP Port 1502)
    - Siemens Logo! Protocol (TCP Port 10001, TCP Port 10005)
    - Siemens S7 Protocol (TCP Port 102)
    - Yokogawa HLLS Protocol (UDP Port 12289, TCP Port 12289)
    - Yokogawa RPS Protocol (UDP Port 12290, TCP Port 12290)

Changed Functionality and Performance Enhancements

The following functionality has been changed in Tenable Network Monitor 5.8.1:

- For Tenable Network Monitor instances connected to Industrial Security, the default Report Frequency has been changed to 5 minutes (from 15 minutes). This ensures a minimal amount of time is required to begin receiving data to IS, and remains a configurable setting from within the UI or from the CLI.
- For all Tenable Network Monitor instances, PII Obfuscation was extended to cover realtime logging and syslog logging. If a detection classified as potentially containing PII reports via either realtime logs or syslogs, the buffer will now be obfuscated by default. In line with changes made in Tenable Network Monitor 5.8.0, this obfuscation can be disabled for stand-alone Tenable Network Monitor instances only. It cannot be disabled for Tenable Network Monitor instances connected to other Tenable products.

For more information about the features and functionality supported in this release, see the Tenable Network Monitor 5.8.x User Guide.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (NEW! Support for RH/CentOS Version 7.6 through kernel version: 3.10.0-957)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Be Advised:

- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.4.1 are supported. Installations running previous versions of Tenable Network Monitor 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to Tenable Network Monitor 5.8.1 - Refer to the Tenable Network Monitor 5.8.0 User Guide for details on upgrading to Tenable Network Monitor 5.8.1.

- Tenable Network Monitor 5.8.1 is compatible with SecurityCenter 4.7.x and later.
- Tenable Network Monitor 5.8.1 is compatible with Industrial Security 1.3.2 and later.
- The Tenable Network Monitor Web Server and Tenable Network Monitor HTML5 User Interface are each automatically updated to version 2.4.1 via a plugin update.

Nessus Network Monitor 5.9.0 Release Notes - 2019-06-03

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

> **Note:** These new features are only available with an Industrial Security subscription and are available only when Tenable Network Monitor is connected to Industrial Security.

New Features

The following are new features included in Tenable Network Monitor 5.9.0:

- Expansion of supported ICS assets to include over 1200 new detections:
  - Badger Meter - Flow Meters (2 new devices)
  - Balluff (34 new devices)
  - Beckhoff - (1000+ new devices)
  - Acromag (172 new devices)
- Expansion of OT Protocol Detections
  - Vnet/IP Basic Protocol & Message Type Detection
- Derivative Detections to Share OT-specific Data with Tenable Security Center
  - OT Protocol Detection
  - OT Vendor Detection

    - OT Family Name Detection
    - OT Model Name Detection
    - OT Model Number Detection
    - OT Serial Number Detection
- Improvements to Existing Detections
    - Optimized OT detections previously only showing up in Plugin Output
    - Added individual device detections for common networking devices (Cisco and Palo Alto)
- Added Default System Types - Discerning what a system is by as much as we know at the moment, including:
    - Host - devices hosting services and using standard IT protocols
    - Endpoint - devices acting as clients and using standard IT protocols
    - ICS Host - devices hosting services and using OT protocols
    - ICS Endpoint - devices acting as clients and using OT protocols

Changed Functionality and Performance Enhancements

The following functionality has been changed in Tenable Network Monitor 5.9.0:

- Stronger Password Protection by storing Cryptographic representations of passwords in the Tenable Network Monitor database.

  (complies with Rule Version (STIG-ID): APSC-DV-001740)

- Tenable Network Monitor recovers when tcp syslog systems get restarted or recover from crashes.

For more information about the features and functionality supported in this release, see the Tenable Network Monitor 5.9.0 User Guide.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.6 through kernel version: 3.10.0-957)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Be Advised:

- Versions of Tenable Network Monitor prior to NNM 5.9.0 will no longer get updates via the feed. This is due to Tenable Network Monitor's web server requiring an upgrade to extend the application's plugins limit. An upgrade to Tenable Network Monitor 5.9.0 is necessary for all prior versions. For most existing customers with web server updates enabled (enabled by default) the transition will be seamless. For a select few customers who (a) have web server updates disabled, (b) have offline versions of Tenable Network Monitor running that do not connect regularly for updates, or (c) customers who download old versions of Tenable Network Monitor and attempt to install them after 30 May 2019, feed updates will no longer work.

  To resolve this, either (1) update using the Tenable Network Monitor 5.9.0 installer/RPM (see User Guide for upgrade instructions) or (2) download the updated web server file (nbin) from the above downloads link, copy it to the `<defaultInstallDir>/var/nnm/scripts/` and restart Tenable Network Monitor.
- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.4.1 are supported.
- Installations running versions prior to Tenable Network Monitor 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to Tenable Network Monitor 5.9.0 - Refer to the Tenable Network Monitor 5.9.0 User Guide for details on upgrading to NNM 5.9.0.
- Tenable Network Monitor 5.9.0 is compatible with SecurityCenter 4.7.x and later.

- Tenable Network Monitor 5.9.0 is compatible with Industrial Security 1.4.0. Note that only specific versions of Tenable Network Monitor are compatible with specific versions of Industrial Security.
- The Tenable Network Monitor Web Server and Tenable Network Monitor HTML5 User Interface are each automatically updated to version 2.5.0 via a plugin update.

Nessus Network Monitor 5.9.1 Release Notes - 2019-07-25

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

> **Note:** These new features are only available with an Industrial Security subscription and are available only when NNM is connected to Industrial Security.

The following are new features included in Tenable Network Monitor 5.9.1:

- Layer 2 protocol detection for the following protocols:
  - LLDP - Link Layer Discovery Protocol
  - Profinet-DCP

Bug Fixes

- Enhanced Security Headers in Tenable Network Monitor UI.
- Fixed issue registering new Tenable Network Monitor scanners to Tenable Vulnerability Management in which jobs from the new scanners would not be uploaded.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit

- Red Hat Linux ES 7 / CentOS 7 64-bit (includes support for RH/CentOS Version 7.6 through kernel version: 3.10.0-957)
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Upgrade Notes

- If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

2018 Tenable Network Monitor

2018 Tenable Network Monitor

Nessus Network Monitor 5.4.1 Release Notes - 3/15/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Features and Improvements

- New detection capability for ICS/SCADA configuration state change
    - All Configuration State & Configuration Change Detection Reporting is Real-Time only to enable leveraging this new detection information from realtime/syslogs.
    - Enhanced existing configuration state & configuration change detections for reporting quality
- Expanded detections for ICS/SCADA protocols
    - Siemens S7+ (New Siemens S7 protocol) Coverage Added
    - Ethernet/IP (Ethernet Industrial Protocol) Detections no longer require TCP Handshake (enabling detection for long-standing sessions)
- Expanded detections for ICS/SCADA asset and vulnerabilities
    - Added New Schneider Electric Device Family Detections:
        - Modicon M340 BMX P34 CPUs
        - Modicon M340 BMX NOR Ethernet/Serial RTU Module
        - Modicon M340 BMX NOR Network Module
    - Expanded existing ICS/SCADA Device/Asset Detections to include additional model #s:
        - Rockwell/Allen Bradley Devices
            - 1756 ControlLogix PLCs – 19 New Models Added
        - Siemens Devices
            - S7-400 PLCs – 11 New Models Added
            - S7-300 PLCs – 25 New Models Added
            - S7-1200 PLCs – 27 New Models Added
            - S7-1500 PLCs – 11 New Models Added
        - Schneider Electric PLCs

- Modicon Premium PLCs – 4 New Models Added
- Modicon Quantum PLCs – 14 New Models Added
- Modicon TSX PLCs – 3 New Models Added

Bug Fixes

- Upgraded Tenable Network Monitor to openssl-1.0.2n.
- Weak Log File Permissions

File Names & Checksums

File	MD5
5.4.1-nnm-5.4.1-es6.x86_64.rpm	365d58c0d4ac0dc62fb73cf96730f193
5.4.1-nnm-5.4.1-es7.x86_64.rpm	9210eb160d36fb379c45096faf88788b
5.4.1-nnm-5.4.1-osx.dmg	f0bccebfb8c66745407ef55f9cf3d5bf
5.4.1-nnm-5.4.1-x64.exe	92ce599871fa2fc153e303867aea48d8
5.4.1-nnm-5.4.1-es5.x86_64.rpm	4c9623410e4d27f69bd381a30c595cb8

Nessus Network Monitor 5.5.0 Release Notes - 5/15/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Features and Improvements

- OT Asset and Vulnerability Detections have been extended to add coverage of the following families of Siemens devices (using the listed industrial protocols). These new capabilities are premium Tenable Network Monitor content, available when Tenable Network Monitor is used as a sensor for Industrial Security.
  - Siemens KTP 700 Family of HMIs (via Siemens S7/S7+ Protocol, SNMP Protocol)
  - Siemens KP 1200 Comfort Family of HMIs (SNMP Protocol, HTTP Protocol)
  - Siemens KP8 Family of HMIs (SNMP Protocol)
  - Siemens S7-200 Family of PLCs (HTTP Protocol)
  - Siemens S7-300 Family of PLCs (SNMP Protocol, HTTP Protocol)
  - Siemens S7-400 Family of PLCs (SNMP Protocol, HTTP Protocol for all models, plus 4 additional models are now supported via Existing S7/S7+ Coverage)
  - Siemens S7-1500 Family of PLCs (21 additional models are now supported via Existing S7/S7+ Coverage)
  - Siemens Logo! Family of PLCs (HTTP Protocol)
  - Siemens ET 200 SP Family of PLCs (SNMP Protocol, HTTP Protocol, Profinet Protocol)
  - Siemens Sinamics G110M Distributed Drive (Ethernet/IP)
  - Siemens Sinamics G120C PN Distributed Drive (Ethernet/IP)
  - Siemens Sinamics CU230P-2 PN Distributed Drive (Ethernet/IP)
  - Siemens Sinamics CU240E-2 PN-F Distributed Drive (Ethernet/IP)
  - Siemens Sinamics G240D-2 PN-F Distributed Drive (Ethernet/IP)
  - Siemens Sinamics G250S-2 PN Distributed Drive (Ethernet/IP)
  - Siemens Sinamics G250D-2 PN-F Distributed Drive (Ethernet/IP)
  - Siemens SIMOCODEproV EIP Motor Management System (Ethernet/IP)
  - Siemens CP 243-1 Ethernet Module (FTP, HTTP)
  - Siemens CP 243-1 IT Ethernet Module (FTP)

    - Siemens CP 343-1 Lean Ethernet Module (FTP)
    - Siemens CP 343-1 Ethernet Module (FTP)
    - Siemens CP 343-1 Advanced Ethernet Module (FTP)
    - Siemens CP 443-1 Ethernet Module (FTP)
    - Siemens CP 443-1 Advanced Ethernet Module (FTP)
    - Siemens SPPA-3000 Control System Detection
    - Siemens T3000 Application and Version Detection
- OT Device Vendor and Model Attributes of a Detected Asset have been populated in many detections and are now visible in the Industrial Security Assets tab.
- IT Detections Added:
    - NTPv4 Server Detection Added
    - Trend Micro OfficeScan Agent Detection Added
    - Trend Micro OfficeScan Server Detection Added
    - Trend Micro OfficeScan Application Information Detection Added

Bug Fixes

- Upgraded OpenSSL to version 1.0.2o.

File Names & Checksums

File	MD5
nnm-5.5.0-es5.x86_64.rpm	8d8a4172729f5513f26dcb752f53ed4a
nnm-5.5.0-es6.x86_64.rpm	90ab948371f07250718f5c3b15f79078
nnm-5.5.0-es7.x86_64.rpm	096f00ac8c084ccd932ea41a48ad8472
nnm-5.5.0-	ed0ae91dbd26f31ba3b5ffd6582e681d

File	MD5
osx.dmg	
nnm-5.5.0-x64.exe	be3ff04cb61550d7ec71a43efd80bef1

Nessus Network Monitor 5.5.1 Release Notes - 6/26/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Upgrade Notes

Note: If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.4.1 are supported. Installations running previous versions of Tenable Network Monitor 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to Tenable Network Monitor 5.5.1 Refer to the Tenable Network Monitor 5.5.1 User Guide for details on upgrading to Tenable Network Monitor 5.5.1.
- Tenable Network Monitor 5.5.1 is compatible with Tenable Security Center 4.7.x and later.
- Tenable Network Monitor 5.5.1 is compatible with Industrial Security 1.1.1.
- The Tenable Network Monitor Web Server and Tenable Network Monitor HTML5 User Interface are each automatically updated to version 2.1.1 via a plugin update.

Supported Platforms

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

What's New

ICS/SCADA (OT) Coverage:

> **Note:** These new capabilities are premium Tenable Network Monitor content, available only when Tenable Network Monitor is used as a sensor for Industrial Security.

- New Device Family Coverage
    - Schneider Electric Device Families (multiple protocols):
        - TSX ETZ 510 Communication Module
        - M221 PLCs
        - M258 PLCs
        - Magelis SCU HMIs
        - Magelis XBT GC/GT HMIs
    - Rockwell/Allen-Bradley Device Families (multiple protocols):
        - Rockwell 1769 CompactLogix 5370 PLCs
        - Rockwell 1768 CompactLogix L4x/L4xS PLCs
    - Expanded Coverage of Existing Families
        - 674 Modbus detections were added to provide more specific coverage of individual industrial controls devices. Detections were added in the following families:
            - Siemens (321 Individual Device Detections added across 31 Device Families)
            - Rockwell/Allen-Bradley (248 Detections added across 28 Device Families)
            - Schneider Electric (105 Detections added across 5 Device Families)

IT Detections Added

Note: These new capabilities are included with Tenable Network Monitor and do not require Industrial Security.

- Nearly 20 new IoT Device Detections were added including devices from:
  - Belkin
  - LIFX
  - TuyaUS
  - Amcrest
  - Samsung SmartThings
  - LogiTech Harmony
  - Geeni
  - Tonbux
  - iSELECTOR
  - Jinvoo
  - Luminea/Pearl
  - Tan Tan
  - Xenon
  - Geekbes

Bug Fixes

- Added DPDK support for RedHat Linux 7.5

File Names & Checksums

File	MD5
5.5.1-nnm-5.5.1-es5.x86_64.rpm	decae1b9a8394c48c2fab184bac5fbb1
5.5.1-nnm-5.5.1-x64.exe	3dfd6044e987fc49ce6cbbb40224b477

File	MD5
5.5.1-nnm-5.5.1-es6.x86_64.rpm	3d10115773a12735235b9995c9763d00
5.5.1-nnm-5.5.1-es7.x86_64.rpm	2bfee5e9e475ca2a3aed55589662609d
5.5.1-nnm-5.5.1-osx.dmg	eda3a24496140fe1ebb8b512c370cb76

Tenable Network Monitor5.6.0 Release Notes - 8/14/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Upgrade Notes

Note: If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.4.1 are supported. Installations running previous versions of Tenable Network Monitor 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to Tenable Network Monitor 5.6.0 - Refer to the Tenable Network Monitor 5.6.0 User Guide for details on upgrading to Tenable Network Monitor 5.6.0.
- Tenable Network Monitor 5.6.0 is compatible with SecurityCenter 4.7.x and later.
- Tenable Network Monitor 5.6.0 is compatible with Industrial Security 1.1.1 and later.
- The Tenable Network Monitor Web Server and Tenable Network Monitor HTML5 User Interface are each automatically updated to version 2.2.0 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit

- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

What's New

ICS/SCADA (OT) Coverage:

> **Note:** These new capabilities are premium Tenable Network Monitor content, available only when Tenable Network Monitor is used as a sensor for Industrial Security.

- 364 new individual ICS device detections across 8 families
    - Schneider Electric Device Families (multiple protocols):
        - Schneider Electric Modicon M258 PLC
- Rockwell/Allen-Bradley Device Families (multiple protocols):
    - 1756-Exxx Ethernet/IP Communications Adapters
    - MicroLogix 1400 PLCs
    - MicroLogix 1400 Communications Adapter
    - GuardLogix 5580 1756-L81E PLCs
    - GuardLogix 5570 1756-L71 PLCs
    - 1756 Armor ControlLogix 5570 PLCs
    - 1789 SoftLogix Software-Defined PLC

IT Detections Added:

> **Note:** These new capabilities are included with Tenable Network Monitor and do not require Industrial Security.

- 22 new IoT Device Detections were added including devices from:
    - D-Link Camera Detections (4)
    - D-Link Home IoT Hub (2)
    - D-Link Smart Door Sensor (1)

  - D-Link Smart Siren (2)
  - D-Link Smart Plugs (2)
  - D-Link Water Sensors (2)
  - Edimax Network Camera (1)
  - Edimax Smart Plug (1)
  - EDNET Smart Camera (1)
  - EDNET Smart IoT Gateway (1)
  - Lightify IoT Bridge (1)
  - Belkin WEMO Insight Switch (1)
  - Belkin WEMO Link (1)
  - Belkin WEMO Switch Smart Plug (1)
  - Withings Body Scale (1)
- Reclassified 18 Printer Detections as IoT System Type

Bug Fixes

- Tenable Network Monitor crashes in HPM when processing reports_reset()

File Names & Checksums

File	MD5
5.6.0-nnm-5.6.0-osx.dmg	58288e4f692c9ae493d9eb56bf16231a
5.6.0-nnm-5.6.0-es5.x86_64.rpm	b9aded1d9d524d19eee3638f76094e15
5.6.0-nnm-5.6.0-es7.x86_64.rpm	15bcd776cc97acb249d963f5b65acda8
5.6.0-nnm-5.6.0-x64.exe	aab6da21dcfe8d747bd887ffec7f4d50
5.6.0-nnm-5.6.0-es6.x86_64.rpm	b23c89f55c7cde760814e764bb022b35

Nessus Network Monitor 5.6.1 Release Notes - 9/25/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features and Changed Functionality

The following are the new features included in Tenable Network Monitor 5.6.1:

- ICS/SCADA (OT) Coverage

  > **Note:** These new capabilities are premium Tenable Network Monitor content, available only when Tenable Network Monitor is used as a sensor for Industrial Security.

  - Over 4,000 new individual ICS device detections across 13 device manufacturers - highlights include:
    - 2679 new Rockwell/Allen-Bradley Device Detections including the following popular families:
      - PLC-5 Series, SLC 500 Series PLCs
      - SmartGuard 600 Series Safety Controllers
      - Rockwell PanelView 5500 Series, PanelView Plus 7 Perf Touch Series & PanelView 800 Series HMIs
    - 734 new Mitsubishi Device Detections including:
      - MELSEC iQ-R Series, Q-Series, L-Series, FX-Series PLCs
      - GOT 1000 Series and GOT 2000 Series HMIs
    - 297 new Panasonic Device Detections, including:
      - FP0R Series, FP0H Series, FP-Sigma Series, FP-X Series, FP-X0 Series, FP-XH Series, FP2sh Series, & FP7 Series PLCs
      - GT Series HMIs
    - 183 new Honeywell Device Detections, including:
      - MasterLogic 200 Series, ControlEdge Series PLCs
- Added support for Windows 10 and Windows Server 2016 64-bit operating systems

- Added support for 10G Tenable Network Monitor on Hyper-V (using currently supported 10G NICs)
- New Software Update Features
  - Enables application updates from the same server that currently delivers plugins, web server and user interface updates (i.e., feed server or Tenable Vulnerability Management).
  - A new configuration for what to update automatically is available in Tenable Network Monitor CLI and Tenable Vulnerability Management Tenable Network Monitor settings (all; web server, HTML client, plugins; plugins only; none).
  - This feature covers stand-alone Tenable Network Monitor and Tenable Vulnerability Management-connected Tenable Network Monitor instances.

Upgrade Notes

- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.4.1 are supported. Installations running previous versions of Tenable Network Monitor 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to Tenable Network Monitor 5.6.1

  Refer to the Tenable Network Monitor 5.6.1 User Guide for details on upgrading to Tenable Network Monitor 5.6.1.
- > **Note:** If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.
- Tenable Network Monitor 5.6.1 is compatible with SecurityCenter 4.7.x and later.
- Tenable Network Monitor 5.6.1 is compatible with Industrial Security 1.1.1 and later.
- The Tenable Network Monitor Web Server and Tenable Network Monitor HTML5 User Interface are each automatically updated to version 2.2.1 via a plugin update.

Bug Fixes and Improvements

The following are the major upgrades and bug fixes included in Tenable Network Monitor 5.6.1:

- Upgrade OpenSSL to 1.0.2p

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

File Names and Checksums

File	MD5
5.6.1-nnm-5.6.1-x64.exe	977011e936e9cc434a0362b46623d8e0
5.6.1-nnm-5.6.1-osx.dmg	0b1ffc432077db89a562beb3b9f278dd
5.6.1-nnm-5.6.1-es6.x86_64.rpm	022a5c6b58b163b3ea9607938f589b81
5.6.1-nnm-5.6.1-es5.x86_64.rpm	1410f28c6b44f3536582afd3061060f8
5.6.1-nnm-5.6.1-es7.x86_64.rpm	98a5c45f7697f138d7fd878a8fe85a18

Nessus Network Monitor 5.7.0 Release Notes - 10/30/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features and Changed Functionality

The following are the new features included in Tenable Network Monitor 5.7.0

Note: For Industrial Security customers, the following new features have been added (this is premium content only available with Industrial Security).

Over 2300 new industrial device detections have been added for the following ICS Device Vendors:

- GE
- Schweitzer
- ABB
- Omron

Device detection is now available within the following industrial protocols:

- DNP3/TCP

Vendor detection is now enabled for all network devices (and visible in the Assets tab of Industrial Security).

> **Note:** Industrial Security users must upgrade IS to 1.2.1 (released concurrently with Tenable Network Monitor 5.7.0). Using Tenable Network Monitor 5.7.0 with earlier versions of IS is not supported.

Upgrade Notes

> **Note:** If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Hyperscan has been upgraded to version 5.0.0
- SQLite has been upgraded to version 3.25.2

Supported Platofrms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

File Names and Checksums

File	MD5
5.7.0-nnm-5.7.0-es5.x86_64.rpm	55f7ed09f46fec5240d180866e605d1a
5.7.0-nnm-5.7.0-es6.x86_64.rpm	7e9fdc3eb4d2be10e509d2c4507977ed
5.7.0-nnm-5.7.0-es7.x86_64.rpm	637ef5d9659bb330bba7605aa0e1dde1
5.7.0-nnm-5.7.0-x64.exe	12df02d41f9aae1067d2ad45351ca369
5.7.0-nnm-5.7.0-osx.dmg	66fe987f84691377392f33663e7456e2

Nessus Network Monitor 5.7.1 Release Notes - 12/19/2018

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features and Changed Functionality

The following are the new features included in Tenable Network Monitor 5.7.1

- Over 600 new ICS devices can now be detected by Tenable Network Monitor when connected to Industrial Security (Premium Content only available with an IS Subscription). These include the following vendors' devices:
  - Fuji (300)
  - Hitachi (150)
  - Toshiba (168)

In addition, the following default functionality has been changed for Tenable Network Monitor in version 5.7.1:

PII Obfuscation Mode has been added as a standard configuration option and by default is now enabled. PII Obfuscation mode was previously an undocumented feature and disabled by default.

- To enable PII Obfuscation Mode, there are two approaches:
  - From the CLI, use the following command:

```
/opt/nnm/bin/nnm --config --add "Enable PII Obfuscation" "1"
```

- From within the Tenable Network Monitor User Interface:
  - Click on the Gear Icon at the top right corner of the Tenable Network Monitor UI and choose Configuration
  - When presented with the Tenable Network Monitor Settings Tab, choose Advanced from the Settings Type dropdown control.
  - The third setting on the Advanced Settings page is the Enable PII Obfuscation field. Setting the field to:

    1 - results in enabling PII Obfuscation.

    0 - results in disabling PII Obfuscation.
- When PII Obfuscation is enabled, all characters of PII detected and displayed in the plugin output will be masked with asterisks (example: *******)
- When PII Obfuscation is disabled, all characters of PII detected and displayed in the plugin output will be unmasked and presented in clear text.

Bug Fixes

- Tenable Network Monitor not respecting proxy settings for Tenable Vulnerability Management Registration

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- MacOS 10.9 - 10.13 64-bit
- Microsoft Windows Vista/7/8/10 and Windows Server 2008/2012/2016 (all 64-bit)

Upgrade Notes

Note: If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Third Party Integrations/Libraries Updated
  - xpLib has been upgraded, including the following component libraries:

    libpcap 1.9.0

    zlib 1.2.11

    libpcre 8.42

2017 Tenable Network Monitor

2017 Tenable Network Monitor

Tenable Network Monitor 5.4 Release Notes - 10/24/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in NNM 5.4.

Upgrade Notes

Note: If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.3.0 are supported. Installations running previous versions of NNM 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to NNM 5.4. Refer to the Tenable Network Monitor 5.4 User Guide for details on upgrading to Tenable Network Monitor 5.4.

- Tenable Network Monitor 5.4 is compatible with Tenable Security Center 4.7.x and later.
- The HTML5 User Interface is automatically updated to version 2.0.0 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- MacOS 10.9 - 10.12 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

File Names & Checksums

File	MD5	SHA1
nnm-5.4.0-es5.x86_64.rpm	be13538b749a9e2caeb413655e2215c2	b87f9640341d120874e461977d6213965622e6a0
nnm-5.4.0-es6.x86_64.rpm	adeb46cccfc3e66edfbbc4febf920acb	04aed04f9741dc8ed32c470372579ad8baaa3c93
nnm-5.4.0-es7.x86_64.rpm	674a19fd48a4c914079f79bfd01ef483	5bc08f80d679c899d27bc03cb75d1bd56905ef22
nnm-5.4.0-osx.dmg	2c06bd50684b50d04b74295d1b221bd3	ab0db4b3fb69b35c988be7383fc4442f9b3d24af
nnm-5.4.0-x64.exe	cedb12e944d9c5665bbfa7c74679b4b4	0e197ddf839025558c98629c2dbc7eaa87498509

What's New

Integration with Gigamon

Use Gigamon's GigaVUE platform to distribute traffic making it easier to scale and extend your Nessus Network Monitor deployment. This includes North-South traffic in the physical infrastructure as well as East-West traffic between and within virtualized servers. Deployed out-of-band, Gigamon's Visibility Fabric aggregates and forwards only the relevant production traffic to Nessus Network Monitors. You can aggregate many taps to a single point or load balance a large stream across many points.

Native integration on APCON IntellaStore

IntellaStore provides complete visibility of both physical and virtual network traffic. The security visibility platform provides traffic aggregation, filtering, and load balancing. IntellaStore can also help pre-optimize traffic before routing to Nessus Network Monitor by deduplication, packet slicing, protocol stripping, and time stamping.

Downstream Integration with Waterfall Unidirectional Gateway

Waterfall Security is a market leader in industrial perimeter unidirectional technology. Unidirectional Gateway appliances provide absolute protection to operational networks from attacks originating on external networks. Nessus Network Monitor seamlessly integrates with Waterfall's Unidirectional Gateway to monitor event data collected from the OT network and published uni-directionally to Tenable Network Monitor.

Enhanced Asset Discovery

Detections for dozens of new asset attributes have been added that increase both breadth and depth of visibility for greater fidelity asset information. Examples include printer detection via TLS/SSL, MAC Address discovery via SNMP and VXLAN, Hostname via DNS and mDNS, and many more.

Additional Improvements

- Upgraded DPDK to 17.05.1.
- Upgraded HyperScan to 4.5.0.
- Upgraded OpenSSL to 1.0.2l.
- "Nessus Network Monitor" name change is now reflected in the product.

Passive Vulnerability Scanner 5.3 Release Notes - 5/16/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in PVS 5.3. A PDF file of these release notes is also available here.

Upgrade Notes

- Upgrades from 4.2.1, 4.4.1, 5.0.0, and 5.2.0 to 5.3.0 are supported. Installations running previous versions of PVS 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to PVS 5.3. Refer to the PVS 5.3 User Guide for details on upgrading to PVS 5.3.

  > **Note:** If your upgrade path skips versions of Nessus Network Monitor, Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- PVS 5.3 is compatible with SecurityCenter 4.7.x and later.
- The HTML5 User Interface is automatically updated to version 1.8.0 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- macOS 10.9 - 10.12 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

File Names & Checksums

File	MD5	SHA1
pvs-5.3.0-es5.x86_64.rpm	021e5ec78f401abe6ad1711c8667d3dd	7a6e76ef4d791ab5bce20afbe9841aa7860e7ea3

File	MD5	SHA1
pvs-5.3.0-es6.x86_64.rpm	9fe9f466a9e13c2b25c0353ce3406c48	6eaa7269b63a7acbb798c0c48da06e3ac73e1269
pvs-5.3.0-es7.x86_64.rpm	878a85883566473e882e60ccb6a87092	7220bdc2c7ee2014044a290a4c6806e43221366e
pvs-5.3.0-osx.dmg	9a54b3a719cd7e7f826ca7d92f7fdc6b	9a9d05288acbbe0e7aa6543f71566e4437ddd75b
pvs-5.3.0-x64.exe	9b031a392579fc3f7371aa744a86103f	c1043ed744ed705e4a82baa5acc6fe47f4cf3c8f

What's New

Improved User Experience with Network Configuration

User experience and the ease-of-use of our products is very important to us. Through user feedback of the PVS experience in SecurityCenter, we found that many users would inadvertently use PVS's default network configuration which could exhaust the user's product license. PVS is now more intelligent to how it suggests default network ranges, which directly addresses the license exhaustion issue. Furthermore, the PVS configuration interface now offers a friendly warning to users who change the network monitoring range to PVS instances managed by SecurityCenter.

Increased Detections in the SCADA/ICS Module

PVS continues to increase detection for ICS/SCADA protocols and devices. PVS can see configuration, status, and health checks based on Modbus network traffic. Furthermore, SCADA device identification was improved through detection of Ethernet/IP network traffic. Through DNP3 network traffic, visibility into configuration activity was added. And lastly, our library of detections has increased its coverage to Rockwell Automation/Allen-Bradley ControlLogix Controller and Module.

Enhanced OS Detection

A key feature to PVS is the added visibility it gives users into their network. This involves both discovery and identification. PVS 5.3 has greatly improved the quality and performance of operating system detection. This will help give PVS users greater detail into the distribution of different operating systems, and their versions, on the network.

Visibility into VXLANs

Virtual Extensible LAN (VXLAN) is a network virtualization technology that addresses scalability problems in large cloud computing deployments. By direct request from our customers, we've added added visibility into VXLAN traffic to the list of PVS capabilities. This continues the theme of PVS empowering customers to gain visibility to all parts of their network, no matter what technology is being used.

Improved PVS 10G performance

The performance of PVS in high performance mode has been improved to be able to process traffic on 10Gbps networks.

Additional Improvements

The OpenSSL version has been updated to 1.0.2k.

2016 Tenable Network Monitor

2016 Tenable Network Monitor

Passive Vulnerability Scanner 5.0 Release Notes - 2/16/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in PVS 5.0. A PDF file of these release notes is also available here.

Upgrade Notes

- The supported upgrade path is from PVS 4.4.x to PVS 5.0. Installations running previous versions of PVS 4.4.x must upgrade to at least 4.4.x prior to upgrading to PVS 5.0. Refer to the PVS 5.0 User Guide for details on upgrading to PVS 5.0.
- PVS 5.0 is compatible with SecurityCenter 4.7.x and later.
- The HTML5 User Interface is automatically updated to version 1.6.0 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

The Microsoft Visual C++ 2010 Redistributable Package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-5.0.0-es5.x86_64.rpm	56a0f25f8ebe73f8acb091be48670a83
pvs-5.0.0-es6.x86_64.rpm	59141a09d4e01ec9f14a6400557ec2d3
pvs-5.0.0-es7.x86_64.rpm	141d18f62a48fbbcf8fcbd6e3e32a015
pvs-5.0.0-osx.dmg	e8dd8a8469bb568b3fb677163aab2ce9
pvs-5.0.0-x64.exe	7d7dfdc158fe0d9644b3cfc72e7510c1

What's New

Improved User Interface

PVS 5.0 includes a much improved interface that provides a summarized dashboard seen after login amongst other new features. The dashboard contains multiple high-level summarized views into hosts, vulnerabilities, applications, operating systems, connections, and mobile devices discovered by PVS. Other additions include:

- A chord diagram is available that visualizes the client connections to servers on well-known ports.
- A network bandwidth chart trends the amount of data sent from client hosts to server hosts and vice versa.
- Improved navigation between client and server hosts, and new pivoting capabilities on any host.
- A Sankey diagram that provides a view of connections between client and server hosts by either host or by network service.

Improved VLAN Monitoring

A new Plugin (ID 19) summarizes all observed VLAN tags for a given host. This helps determine if a host has switched VLANs or is present on an incorrect or unexpected VLAN.

Detection and Analysis of Tunneled IPv6 Traffic

In addition to reporting the presence of tunneled IPv6 traffic, PVS now processes the IPv6 traffic within the tunnel. Teredo, 6to4, and 6in4 tunnel detections are now summarized in a single plugin (ID 20) and other detections will be associated to the IP addresses found within the tunneled traffic.

Increased Analysis of IPv6 Traffic

PVS now detects the presence of IPv6 headers and performs a complete analysis of IPv6 packets that contain extension headers.

Discovery of Applications within Encrypted Traffic

PVS increases application visibility by using TLS fingerprinting to discover applications whose traffic is encrypted.

Extended Packet Filtering

PVS provides more targeted packet filtering by extending its BPF filter support.

Additional Improvements

- Added HTTP Strict Transport Security (HSTS) headers to the PVS Web Server.
- Replaced initial certificates signed with the SHA1 hashing algorithm with certificates signed with SHA-256.
- PVS now displays both successful and unsuccessful last logon attempts immediately after login. Previously, only unsuccessful attempts were shown.
- Fixed an issue where SecurityCenter would continually report PVS status as "Updating Plugins".
- Extended an interval after which PVS needs to be reactivated if it has not received plugin updates from SecurityCenter during that interval. The interval has been extended from 14 days to 30 days.
- Replaced a PASL (ID 7043) with an internal plugin (ID 18) for summarized reporting of protocols used by hosts.
- Upgraded OpenSSL to 1.0.2f.

Passive Vulnerability Scanner 4.4.1 Release Notes - 3/24/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This version of PVS upgrades OpenSSL to 1.0.2g and fixes an issue where the the status of PVSs managed by SecurityCenter could remain in the "Updating Plugins" state.

Upgrade Notes

- Refer to the PVS 4.4 User Guide for details on upgrading to PVS 4.4.1.
- PVS 4.4.1 is compatible with SecurityCenter 4.7.x and later.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit

- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

The Microsoft Visual C++ 2010 Redistributable Package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.4.1-es5.x86_64.rpm	8862c5b402d686363f8c3d396f7fc905
pvs-4.4.1-es6.x86_64.rpm	068f3fa9afc904d187bf75839409a6f2
pvs-4.4.1-es7.x86_64.rpm	c2e7a808c0956f870c2119ad4c3459ef
pvs-4.4.1-osx.dmg	0b5e6690cac217a05c99841efaba6b28
pvs-4.4.1-x64.exe	6a1c5900c825c07ea3e2cc4b4e8d66ff

Passive Vulnerability Scanner 5.1 Release Notes - 6/14/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in PVS 5.1. A PDF file of these release notes is also available here.

Upgrade Notes

- Upgrades from 4.2.1, 4.4.1, and 5.0.0 to 5.1.0 are supported. Installations running previous versions of PVS 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to PVS 5.1. Refer to the PVS 5.1 User Guide for details on upgrading to PVS 5.1.
- PVS 5.1 is compatible with SecurityCenter 4.7.x and later.
- The HTML5 User Interface is automatically updated to version 1.7.0 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

The Microsoft Visual C++ 2010 Redistributable Package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-5.1.0-es5.x86_64.rpm	a49172d648f0fb3013d117f2c525757c
pvs-5.1.0-es6.x86_64.rpm	1b227a2723766318db78850edb276d4f
pvs-5.1.0-es7.x86_64.rpm	74d4c704dcfa970404b24aa007247eee
pvs-5.1.0-osx.dmg	1497d087b4df0eaa8c35eab5321d18b0
pvs-5.1.0-x64.exe	c6344d6d138999e99de13b3d53155a35

What's New

- **Improved Hostname and MAC Address reporting:** The existing DHCP-based hostname and MAC address detection has been included in augmenting PVS's host properties reporting.
- **Ability to import known hosts:** A list of known hosts can be imported into PVS to avoid PVS reporting them as new hosts.
- **Ability to combine PCAP reports:** The PVS client allows the user to upload multiple PCAPs at once so that their results can be combined into a single PCAP report. The maximum size of one or more PCAPs that can be uploaded has been increased to 100 MB.
- **Improved management of lifetime of hosts:** PVS now supports a new configuration parameter "Host Lifetime" for the lifetime period of hosts. This would allow for hosts to be retained for a longer period of time than vulnerabilities.

- **Support for limiting PVS communication to TLS 1.2 or higher:** VS Web Server communication can be configured to be limited to TLS 1.2 or higher.
- **Improved custom plugin management:** The PVS client provides the ability to delete custom plugins.

Additional Improvements

- PVS client now displays both successful and unsuccessful last logon attempts immediately after login.
- PVS includes an option to recover a PVS SQLite database if it becomes malformed.
- The Web Server and HTML Client files are updated only if their versions in the feed are newer than their corresponding versions on PVS.
- PVS can be directly upgraded from 4.2.1 and 4.4.1 to 5.1.0.
- PVS client shows the filename of the PCAP processed.
- CPE information is available in the Vulnerabilities details view of the PVS client.
- Upgraded DPDK to 2.2.
- Upgraded SQLite to 3.11.1.
- Upgraded OpenSSL to 1.0.2h.

Passive Vulnerability Scanner 5.2 Release Notes - 12/12/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in PVS 5.2. A PDF file of these release notes is also available here.

Upgrade Notes

- Upgrades from 4.2.1, 4.4.1, and 5.0.0 to 5.2.0 are supported. Installations running previous versions of PVS 4.2.1 must upgrade to at least 4.2.1 prior to upgrading to PVS 5.2. Refer to the PVS 5.2 User Guide for details on upgrading to PVS 5.2.
- PVS 5.2 is compatible with SecurityCenter 4.7.x and later.
- The HTML5 User Interface is automatically updated to version 1.8.0 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- macOS 10.9 - 10.12 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

File Names & MD5 Checksums

File	MD5
pvs-5.2.0-es5.x86_64.rpm	14a78600769825d3a9f047b006f22c5d
pvs-5.2.0-es6.x86_64.rpm	abbb0eea84e0522fef5c269d45de1bfd
pvs-5.2.0-es7.x86_64.rpm	19e7904fa769f5f1a1ca3659b4b6066e
pvs-5.2.0-osx.dmg	86ac1eb1ffa907cd667455d3088540d5
pvs-5.2.0-x64.exe	40b17d33954ed1a3c26f4daa9cdea461

What's New

New SCADA Analysis Module

PVS includes a new analysis module that analyzes SCADA network traffic to discover SCADA assets and their vulnerabilities. This module provides the same capabilities as SCADA plugins that are loaded by PVS versions older than 5.2, with improved performance. In addition, the module provides deep visibility into the type of SCADA devices discovered. This module is enabled by default and can be disabled in environments that do not contain SCADA devices.

New SCADA Top-N charts

The following charts have been added to the dashboard in the PVS client and provide a high-level summary of SCADA assets, their vulnerabilities, and protocols used by them. The charts are disabled by default.

1. SCADA Vulnerability Distribution by Severity
2. Top 10 SCADA Hosts

3. SCADA Host Distribution by Protocol
4. SCADA Host Distribution by System Type

New Connection Analysis Module

The connection reporting features of the Tenable Network Monitor (TNM) are now available within PVS as part of a new Connection Analysis module. This module eliminates the need for TNM to obtain connection duration and bandwidth information, and extends the platform support to all platforms supported by PVS. Connection duration and bandwidth reporting for IPv6 and tunneled traffic is a new addition and also available with this module. This module is disabled by default.

Improved PVS 10G performance

PVS now uses a new high-performance regular expression matching library for pattern matching when analyzing network traffic in high performance mode.

Improved VLAN reporting for hosts

PVS includes the ID of the VLAN a host lies within, in the report sent to SecurityCenter. The PVS client includes support for a user to query hosts by VLAN ID and also reports the VLAN ID within the host's detail view.

Support for macOS 10.10, 10.11, and 10.12

PVS 5.2.0 supports macOS versions 10.9 to 10.12.

Additional Improvements

- HTML reports now include an option to include an Executive Summary chapter. This chapter contains the following sub-sections: Top 10 Vulnerabilities by Count, Top 10 Most Severe Vulnerabilities, Top 10 Hosts with Most Severe Vulnerabilities, and Hosts with Obsolete Operating Systems.
- Fixed an issue where PVS may stop processing packets in High Performance Mode (10G PVS) in a VM deployment on high bandwidth networks.
- The Events view in the PVS client includes byte transfer size details for connection events.
- The number of worker threads can be configured to a maximum of 16 in high performance mode.
- The SQLite version used by PVS has been upgraded to 3.13.0.
- The OpenSSL version used by PVS has been upgraded to 1.0.2j.

- The jQuery UI version used by PVS has been upgraded to 1.12.0.
- The Expat version used by PVS has been upgraded to 2.2.0.

2015 Tenable Network Monitor

2015 Tenable Network Monitor

Passive Vulnerability Scanner 4.2 Release Notes - 1/28/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in PVS 4.2 and HTML5 User Interface 1.3. A PDF file of these release notes is also available here.

Upgrade Notes

- Refer to the PVS 4.2 User Guide for details on upgrading to PVS 4.2.
- PVS 4.2 is compatible with SecurityCenter 4.6 and later.
- The HTML5 User Interface is automatically updated to 1.3 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit

- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

Support for 32-bit systems has been dropped in 4.2.

The Microsoft Visual C++ 2010 Redistributable Package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.2.0-es5.x86_64.rpm	b58d299a3a21517218efe226186ada2f
pvs-4.2.0-es6.x86_64.rpm	e99cad3e2640f156dc7b5ca822f83c72
pvs-4.2.0-x64.exe	d76bafaf8afca274edcce8f37662180a
pvs-4.2.0-osx.dmg	995d40ab4df871c500cbc41305c1cd2a

What's New

- **Top-N Dashboard**: Easy, high-level visibility into Top-N hosts, vulnerabilities, applications, operating systems and connections via multiple canned charts and ability to add custom charts.
- **Real-time Event Analysis View**: The PVS HTML5 user interface contains a new real-time event analysis dashboard of real-time events generated by PVS.
- **Syslog generation in CEF format**: Syslog messages can be generated in the CEF format in addition to the standard format.
- **Syslog forwarding over TCP**: Syslog messages can be forwarded either over UDP or TCP.
- **TNM-style session logging**: Support for new syslog message that contains TCP session information.
- **PVS configuration updates without restart**: A restart of PVS is no longer needed after changing the PVS configuration.
- **Import PCAP files via HTML5 User Interface**: Users can import PCAP files via the HTML5 User Interface.
- **Snapshot comparison**: Quick comparison of changes between two monitoring snapshots.

- **Improved Plugin Management**: Easier management of plugins via HTML5 User Interface.
- **Change to Licensing**: Removed license key requirement when PVS is being managed by SecurityCenter.

Additional Improvements

- Added complexity checks for passwords.
- Added ability to configure maximum sessions per user and maximum number of login attempts.
- Added ability to display a customizable login banner in the PVS HTML5 User Interface.
- Added ability to reset PVS user passwords.
- Added ability to view additional network interface details in the PVS HTML5 User Interface.
- Upgraded libpcap to 1.5.3 for Linux versions.
- Upgraded SQLite to 3.8.6.
- Upgraded OpenSSL to 1.0.0p.

Passive Vulnerability Scanner 4.0.4 Release Notes - 2/12/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This version of PVS upgrades OpenSSL to 1.0.0q.

Note: Some customers may notice that a HTML5 client user is logged out after accessing the Configuration page. This issue applies to 4.0.4 only and has been addressed with a plugin update. A manual plugin update may be necessary if the plugins have not been updated automatically.

Upgrade Notes

- PVS 4.0 will automatically import configuration from pvs.conf and pvs-proxy.conf into a database. More details are available in the PVS 4.0 User Guide.
- Copy the existing PVS license key file from the existing PVS to the workstation the initial setup will be completed from as the key will be requested during completion of the setup wizard
- PVS 4.0 is compatible with SecurityCenter 4.6 and later.

Stop the PVS daemon before performing the upgrade:

```
# /etc/init.d/pvs stop
```

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 32/64-bit
- Red Hat Linux ES 6 / CentOS 6 32/64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 32/64-bit

The Microsoft Visual C++ Redistributable package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.0.4-x64.exe	ab094fe91f187b3c29fa75e9f4b1502d
pvs-4.0.4-es5.i386.rpm	9588d68cb1234f0df0bec9f4c54f9fd4
pvs-4.0.4-es5.x86_64.rpm	8e4327d41c0993338a17418f904aa0a3
pvs-4.0.4-es6.i386.rpm	40692266238c9d93c2e36ea43cee9159
pvs-4.0.4-es6.x86_64.rpm	95699663ce166cb51136accb884b3ed4
pvs-4.0.4-i386.exe	2c36bd88c869993a320b056356755450
pvs-4.0.4-osx.dmg	59f60398d09cbfe4892309d4d6ce5a89

Passive Vulnerability Scanner Web Server 1.3.1 Release Notes - 2/12/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

An updated version of the PVS Web Server (version 1.3.1) was pushed into the feed today. This fixed a compatibility issue with PVS 4.0.4 due to which user is logged out of the HTML5 client after accessing the Configuration page. This issue applies to PVS 4.0.4 only.

Passive Vulnerability Scanner 4.2.1 Release Notes - 4/28/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in PVS 4.2.1 and HTML5 User Interface 1.3.1. A PDF file of these release notes is also available here.

Upgrade Notes

- Refer to the PVS 4.2 User Guide for details on upgrading to PVS 4.2.1.
- PVS 4.2.1 is compatible with SecurityCenter 4.7.x and later.
- The HTML5 User Interface is automatically updated to 1.3.1 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

Support for 32-bit systems has been dropped in 4.2.

The Microsoft Visual C++ 2010 Redistributable Package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.2.1-es5.x86_64.rpm	7a42eb0898509a7d4fb948fa956c15f2

File	MD5
pvs-4.2.1-es6.x86_64.rpm	5c90f04ed6fe4e606f2792f55209c859
pvs-4.2.1-es7.x86_64.rpm	128791723f36b3f79406720b9a663375
pvs-4.2.1-osx.dmg	22b26286ab7744a8093ec7bcc596d86b
pvs-4.2.1-x64.exe	9f9710af98fbb9f54299274414647b1e

What's New

10Gbps Support for Virtual/Software deployments (Non Tenable Appliance)

PVS version 4.2.1 provides capabilities for real-time multi-gigabit network traffic monitoring for software-based installs either with bare-metal installs of RHEL 6 or running under VMware ESX/ESXi 5.5.

ERSPAN Encapsulation Support

In addition to Generic IP Encapsulation, added support for VMware ERSPAN (Transparent Ethernet Bridging) and Cisco ERSPAN (ERSPAN Type II). ERSPAN allows you to mirror traffic from one or more "source" ports on a virtual switch or even a physical switch or router and send the traffic to a "destination IP" host running PVS. This could help in situations were provisioning a span port or network tap is problematic. More general info on ERSPAN:

http://blogs.vmware.com/vsphere/2013/02/vsphere-5-1-vds-feature-enhancements-port-mirroring-part-3.html

Red Hat 7 Support for standard mode (non 10Gb)

Standard mode PVS is now supported on RHEL 7. High speed (10G mode) will be supported in a future release.

License enforce throughput by entitlement ("Standard mode" vs 10G "High speed mode")

High speed (10G mode) is now enforced via activation code. SC-CV includes unlimited "standard mode" PVS but each 10G sensor will need a dedicated activation code.

Additional Improvements

- Realtime session logging has been updated to included total bytes transferred and session duration.

- Prevent interfaces that have IP addresses bound to them from being selected in high performance mode.
- Upgraded SQLite to 3.8.8.3.
- Upgraded OpenSSL to 1.0.0r.

Passive Vulnerability Scanner 4.4.0 Release Notes - 9/8/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes the new features and improvements that are introduced in PVS 4.4.0. A PDF file of these release notes is also available here.

Upgrade Notes

- Refer to the PVS 4.4 User Guide for details on upgrading to PVS 4.4.0.
- PVS 4.4.0 is compatible with SecurityCenter 4.7.x and later.
- The HTML5 User Interface is automatically updated to version 1.4.0 via a plugin update.

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Red Hat Linux ES 7 / CentOS 7 64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 64-bit

The Microsoft Visual C++ 2010 Redistributable Package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.4.0-es5.x86_64.rpm	3f0278719dcef9d4777a8a8d6f35b5db

File	MD5
pvs-4.4.0-es6.x86_64.rpm	7265448e4e07e4018ffb1b060c2c38ff
pvs-4.4.0-es7.x86_64.rpm	245ef6c510ac1786ae637f35aab9cc10
pvs-4.4.0-osx.dmg	62b863e90cf5781881bb39f3fd9990d9
pvs-4.4.0-x64.exe	1ce696d8a886413e88399b193330983a

What's New

- **Support for launching basic network Nessus scan** - PVS 4.4.0 provides the ability to launch an active basic network Nessus scan on hosts monitored by PVS. This feature integrates with Nessus 6.4 or above, as it requires API keys.

- **New results views and charts for Mobile devices** - New Mobile results views have been added to the user interface that provide visibility into mobile devices discovered and their attributes such as device model and operating system, their vulnerabilities and applications discovered running on them. A few distribution charts by device model, operating system and mobile applications have also been added.

- **Support for email notifications containing a summary of monitored results** - Email notifications can be configured and sent that contain summarized reports of discovered hosts, vulnerabilities, applications and operating systems.

- **Red Hat 7 support for High Performance mode (10 Gbps)** - High Performance mode PVS is now supported on RHEL 7.

- **Support for CVSS v3.0** - PVS supports the new vectors and scores introduced in CVSS v3.0.

- **Support for DNS hostnames and NETBIOS name reporting** - PVS can now use reverse DNS lookups to determine the hostname for monitored hosts. The DNS lookups are enabled by default and can be disabled by setting the "DNS Queries Per Interval" parameter to 0. The DNS hostnames and NETBIOS names are reported in .nessus reports. The ability to view the hostname in the user interface will be available in a future release.

Additional Improvements

- Added the ability to switch the performance mode from the user interface.

- Improved the realtime events view in the user interface.

- Lock user interface user accounts only if the maximum number of failed login attempts has been exceeded over a 24-hour period.
- Fixed an issue where SecurityCenter would continually report PVS status as "Updating Plugins".
- Upgraded SQLite to 3.8.10.2.
- Upgraded OpenSSL to 1.0.2d.

2014 Tenable Network Monitor

2014 Tenable Network Monitor

Passive Vulnerability Scanner 4.0.1 Release Notes - 1/29/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The document describes the changes that are introduced in PVS 4.0.1, as well as significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- PVS 4.0 will automatically import configuration from pvs.conf and pvs-proxy.conf into a database. More details are available in the PVS 4.0 User Guide.
- Copy the existing PVS license key file from the existing PVS to the workstation the initial setup will be completed from as the key will be requested during completion of the setup

wizard

- PVS 4.0 is compatible with SecurityCenter 4.6 and later.

Stop the PVS daemon before performing the upgrade:

```
 # /etc/init.d/pvs stop
```

The command syntax for an RPM upgrade is as follows:

```
 # rpm -Uvh [RPM Package File Name]
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 32/64-bit
- Red Hat Linux ES 6 / CentOS 6 32/64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 32/64-bit

The Microsoft Visual C++ Redistributable package is a prerequisite which needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.0.1-es5.i386.rpm	dd6fa5b45f56672221eda1b3b53caaaa
pvs-4.0.1-es5.x86_64.rpm	fda285ab12867be218b74697881f8de9
pvs-4.0.1-es6.i386.rpm	f1c772ff26462d1cc7fa1375a63f40a5
pvs-4.0.1-es6.x86_64.rpm	512f8f7996a44682cb87228dbe3ed724
pvs-4.0.1-i386.exe	d819de511ae4f35ccc5365edebb44f8c
pvs-4.0.1-x64.exe	78bb25ec014e1cc2ad028d5faf987a1d
pvs-4.0.1-osx.dmg	3cd910520a5d165b344e9b0690a47658

What's New

- License Change: Removed the 16 IP limit for evaluation and now provide a full product evaluation for 30-days
- Added new OS platform support for Mac OS X 10.8 and 10.9
- Added new result filtering options for CPE, IAVM, and STIG Severity
- Added reporting of the confidence level and detection method to OS Fingerprinting plugin output
- Logs failed / successful login attempts to the admin log
- Changed the syslog format for Encrypted/Interactive sessions to match the other internally generated events
- Adds a connection count to the plugin output for internal client/server connection summary
- Improved resource utilization
- Expanded the size of the input field for monitored networks
- Added plugin output to real-time PASL syslog
- Fixed an issue when monitoring inactive interfaces that stopped monitoring
- Fixed an issue that generated a malformed report which would fail to import into SecurityCenter
- Fixed an issue on upgrades that did not import the syslog host and vlan settings correctly

PVS Web Server / Client UI Changes

These are not specific to 4.0.1:

- Added a link in the application and operating system tabs to enable pivoting back to a list of vulnerabilities for a given host
- Changed to reflect the new Nessus severity color scheme
- Added support for UI classification banners

Passive Vulnerability Scanner 4.0.2 Release Notes - 4/2/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The document describes the changes that are introduced in PVS 4.0.2, as well as significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- PVS 4.0 will automatically import configuration from pvs.conf and pvs-proxy.conf into a database. More details are available in the PVS 4.0 User Guide.
- Copy the existing PVS license key file from the existing PVS to the workstation the initial setup will be completed from as the key will be requested during completion of the setup wizard
- PVS 4.0 is compatible with SecurityCenter 4.6 and later.

Stop the PVS daemon before performing the upgrade:

```
 # /etc/init.d/pvs stop
```

The command syntax for an RPM upgrade is as follows:

```
 # rpm -Uvh [RPM Package File Name]
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 32/64-bit
- Red Hat Linux ES 6 / CentOS 6 32/64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 32/64-bit

The Microsoft Visual C++ Redistributable package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.0.2-es5.i386.rpm	6be15eeb78655386f493925418407921
pvs-4.0.2-es5.x86_64.rpm	04d3e7af265d7d8deba25894ca3077c5
pvs-4.0.2-es6.i386.rpm	8ca438db87f220d5dddd70224bf5998a

File	MD5
pvs-4.0.2-es6.x86_64.rpm	1a0748c1954805a2b346ceaeb90e5535
pvs-4.0.2-i386.exe	b077b071906c4b8472544699a4f0765a
pvs-4.0.2-x64.exe	05e3a78a0ce2d4dae39afc4ffe0e2aba
pvs-4.0.2-osx.dmg	411fbf1dff9145f9f607e6837c4219c6

What's New

Includes the following improvements and bug fixes:

- Expired PVS licenses or activation codes now returns the user to the Quick-Setup wizard to allow a new license to be entered
- The "External Access" tag was missing from hosts with Internet facing vulnerabilities. This has been added into the plugin output
- Relaxed the Password complexity requirements on the Web Proxy Password setting
- Relaxed the port setting restrictions for "Web Proxy Port" to allow ports below 1024 to be specified
- Fixed a filtering issue on the "Affected Host List"
- Fixed a dependency issue that caused some PASL script false positives
- Made multiple improvements to the plugin evaluation logic
- Removed non-printable characters from the data provided from some PASL scripts

Passive Vulnerability Scanner UI 1.2 Release Notes - 4/24/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

An updated version of the PVS user interface (version 1.2) was pushed into the feed today. This new version scales better, is easier to use, and has an improved look and feel.

The new UI has adopted some of the Nessus UI 2.x navigational improvements so that the client looks and operationally feels similar to the Nessus client.

The following are the other improvements made:

- Added table column headers in the Vulnerabilities, Applications, Operating Systems, and Connections views to enable sorting of vulnerabilities by different criteria
- Improve loading time for large reports
- Introduced Notification Center - provide access to historical notifications
- Enhanced usability on mobile devices
- Improved process of applying a PVS license key when PVS is used with SecurityCenter.

This update is being distributed through a plugin update, no upgrade necessary. The browser cache may need to be cleared and the browser refreshed to view the new client.

Passive Vulnerability Scanner Web Server 1.1.3 Release Notes - 5/1/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

An updated version of the PVS Web Server (version 1.1.3) was pushed into the feed today. This version includes the following fixes and improvements:

- Added additional protections against non-printable characters from being stored in the PVS database.
- Fixed filtering issues when filtering by CVSS score with certain values.
- Improved query performance for the Applications and Operating Systems tabs.

This update is being distributed through a plugin update and no upgrade is necessary.

Passive Vulnerability Scanner 4.0.3 Release Notes - 6/12/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This version of PVS upgrades OpenSSL to 1.0.0m to address SSL/TLS MITM vulnerability (CVE-2014-0224).

Upgrade Notes

- PVS 4.0 will automatically import configuration from pvs.conf and pvs-proxy.conf into a database. More details are available in the PVS 4.0 User Guide.

- Copy the existing PVS license key file from the existing PVS to the workstation the initial setup will be completed from as the key will be requested during completion of the setup wizard
- PVS 4.0 is compatible with SecurityCenter 4.6 and later.

Stop the PVS daemon before performing the upgrade:

```
 # /etc/init.d/pvs stop
```

The command syntax for an RPM upgrade is as follows:

```
 # rpm -Uvh [RPM Package File Name]
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 32/64-bit
- Red Hat Linux ES 6 / CentOS 6 32/64-bit
- Mac OS X 10.8 and 10.9 64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 32/64-bit

The Microsoft Visual C++ Redistributable package is a prerequisite that needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.0.3-es5.i386.rpm	4ada80893dbe51d65f12231ab025f145
pvs-4.0.3-es5.x86_64.rpm	a6f9b1cc7c4ce29b48b1d1a1e593e4a6
pvs-4.0.3-es6.i686.rpm	3300f2a74750ab1f7c3fe29910d24975
pvs-4.0.3-es6.x86_64.rpm	5980cda1958ed8e9507b74aefd23e2fc
pvs-4.0.3-i386.exe	9b53139d6542e893fc5464819bb64dc5
pvs-4.0.3-x64.exe	73e877ba0a83cffa6c5ce56aac2607fc
pvs-4.0.3-osx.dmg	7d7cc3679a00ea67a79a742c90361f52

2013 Tenable Network Monitor

2013 Tenable Network Monitor

Passive Vulnerability Scanner 3.8.1 Release Notes - 2/28/2013

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The document describes the changes that are introduced in PVS 3.8.1, as well as significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

If you were running PVS 3.8.0 previously with hosts backup file ("backup-file") enabled, it is recommended that you remove the /opt/pvs/var/pvs/pvs-hosts.bin file. This will improve the initialization process and allow PVS to rediscover the hosts on the network.

Stop the PVS daemon before performing the upgrade:

```
# /etc/init.d/pvs stop
```

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 32/64-bit
- Red Hat Linux ES 6 / CentOS 6 32/64-bit
- Windows Server 2008 32/64-bit
- Windows 7 32/64-bit

The Microsoft Visual C++ Redistributable package is a prerequisite which needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-3.8.1-es5.i386.rpm	49ea321f79ef297a2ddd022897898a60
pvs-3.8.1-es5.x86_64.rpm	8f5f8582c2470e9184639c8240a767e0
pvs-3.8.1-es6.i386.rpm	1f6c49f866546e82c2c900f1d24026cc
pvs-3.8.1-es6.x86_64.rpm	166422ba00310f59938fff7e8252434a
pvs-3.8.1-i386.exe	7b1f4ff5c77a61fcbe63a8f93752c303
pvs-3.8.1-x64.exe	952ceb966373b63248a3c2a7bb263f6c

Connection Tracking Enhancements

Improved reporting on connections between hosts and ports. For PVS, a connection is any unique combination of a source IP, destination IP, and a destination port.

Plugin 3 - "Internal Client Trusted Connection"

Plugin 3 has been renamed from "Show connections" to "Internal Client Trusted Connection". The functionality has changed to now include a summary of all internal servers that a particular host has connected to on a port. The summary is limited to only display the last 1,000 addresses but also provides a count of the total number of hosts.

Plugin 15 - "Internal Server Trusted Connection"

Plugin 15 has been renamed from "Server Connection" to "Internal Server Trusted Connection". This plugin is essentially the opposite of plugin ID 3 as it displays all client systems that have connected to a server on a particular port. The functionality of this plugin has also changed to report a summary of connections with a total count.

New Plugin 16 - "Outbound External Connection"

Plugin 16 is a new plugin that has been added to help identify outbound connections from the monitored network. The plugin identifies which systems are connecting outbound and which destination ports they are connecting outbound to.

Additional Improvements

- Updated OpenSSL to 1.0.0k (includes security fixes for CVE-2013-0169, CVE-2013-0166)
- Security improvements include more secure Windows configuration and digitally signed all remaining binaries.
- ContinousView licenses now include support for IPv6 monitoring

Bug Fixes

- Corrected an IP range calculation error that occurred when the monitored ranges specified was a subset of the licensed range.
- Fixed an issue that reported on IP addresses outside of the monitored range.

Passive Vulnerability Scanner 4.0 Release Notes - 9/12/2013

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The document describes the changes that are introduced in PVS 4.0, as well as significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

- PVS 4.0 will automatically import configuration from pvs.conf and pvs-proxy.conf into a database. More details are available in the PVS 4.0 User Guide.
- Copy the existing PVS license key file from the existing PVS to the workstation the initial setup will be completed from as the key will be requested during completion of the setup wizard
- PVS 4.0 is compatible with SecurityCenter 4.6 and later.

Stop the PVS daemon before performing the upgrade:

```
# /etc/init.d/pvs stop
```

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 32/64-bit
- Red Hat Linux ES 6 / CentOS 6 32/64-bit
- Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 32/64-bit

The Microsoft Visual C++ Redistributable package is a prerequisite which needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-4.0.0-es5.i386.rpm	369f5228cbc3d100ca6b6c3a2eee86fc
pvs-4.0.0-es5.x86_64.rpm	d1be1bc30b4cdff12cb0bae9b4ed0c16
pvs-4.0.0-es6.i386.rpm	030fb600692a2c25b6c5b4bef91dba31
pvs-4.0.0-es6.x86_64.rpm	f9e35cc308330ad411419e1f96f45a04
pvs-4.0.0-i386.exe	f2ec2b9623ab7a79b312ccb9799afa75
pvs-4.0.0-x64.exe	2e61da2ad0e5b6e0ecf7a1ced3fdb49e

What's New

- **New User Interface** - a new HTML5 web based interface, similar to the Nessus HTML front-end, for configuration, management, and reporting allows PVS to be utilized in a stand-alone mode
- **Simplified installation** - After installation point your web browser to https://[ip address]:8835 to perform the initial configuration through a quick setup wizard. Then explore the new interface and complete further configuration options as needed.
- **Reporting on live monitored traffic** - Easy and detailed visibility into discovered hosts, vulnerabilities, applications, connections, and operating systems in real-time
- **Web-based data export** - multiple file formats (.csv, .nessus, .html) supported
- **Automatic snapshots** - network discovery and vulnerability data provides visibility into changes over time

Additional Improvements

- PVS now ciphers all of the report and configuration data
- The use of pvs.conf and pvs-proxy.conf is now deprecated in favor of a sqlite-based database (config.db).
- Support for plugin feed activation codes allows for new annual subscription based license options
- Support for automatic updates of PVS Web Server and PVS HTML Client in stand-alone mode.
- Uses Nessus (NASL) web server and similar RESTful API. The list of web API calls will be added to the documentation in the near future.
- Ability to upload and browse reports from PVS 3.6 and later
- Command line options to register and configure PVS, and update plugins
- Added support for vulnerabilities with a critical severity
- Reduced memory footprint
- Added complexity checks for passwords
- Added support for Windows 8 and Windows Server 2012
- Upgraded libpcap to 1.4.0 for Linux versions and WinPcap to 4.1.3 for Windows versions

2012 and Earlier Tenable Network Monitor

2012 and Earlier Tenable Network Monitor

Passive Vulnerability Scanner 3.0.2 Release Notes

Passive Vulnerability Scanner 3.0.3 Release Notes

Passive Vulnerability Scanner 3.0.4 Windows Release Notes

Passive Vulnerability Scanner 3.2.0 Release Notes

Passive Vulnerability Scanner 3.4.0 Release Notes

Passive Vulnerability Scanner 3.6.0 Release Notes

Passive Vulnerability Scanner 3.8.0 Release Notes - 12/4/2012

2012 and Earlier Tenable Network Monitor

Passive Vulnerability Scanner 3.0.2 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

General:

- An issue existed where the same alert would be reported multiple times.
- PVS and PVS Proxy services startup scripts would incorrectly report successful or failed attempts to start these services.
- Corrected reported issues with plugins 3829 and 3830.
- Added new functionality in the form of being able to identify hosts that accept connections from outside of the protected network.

Windows:

- Several minor improvements to installation and the GUI.
- Several reported issues in the GUI display, as well as the reports have been corrected.

Passive Vulnerability Scanner 3.0.3 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This version of PVS corrects an issue surrounding the execution of the highest numbered plugin that is in the application. Essentially, if the highest numbered plugin were to trigger, it would cause PVS to fail. The highest numbered plugin will change as new plugins are released and plugins updates are performed on PVS scanners.

Passive Vulnerability Scanner 3.0.4 Windows Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This version of PVS Windows contains an updated version of WinPcap due to a security issue found within the older version of WinPcap.

Passive Vulnerability Scanner 3.2.0 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in PVS version 3.2.0, the significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

General Notes

As with any application, it is always advisable to perform a backup of the installation before upgrading.

Supported Platforms

Support is available for Red Hat ES 3, ES 4, ES 5 and CentOS 5 64-bit.

Upgrading from 3.0.x

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh <RPM Package File Name>
```

Application Notes

New Features

- Passive Analysis Scripting Language (PASL)
- OS fingerprinting is now based on SinFP (formerly based on p0f) - uniform with Nessus
- Ability to exclude IP addresses/ranges from being monitored
- Support for non-TCP/non-UDP packet analysis - 21 new protocols supported
- Detect and report external accessibility of vulnerabilities
- New output formats: XML, Nessus and HTML

Passive Analysis Scripting Language (PASL)

PASL is a scripting language (Similar to NASL and TASL) that provides the following functionality over existing PRMs:

- Perform advanced analysis of network packets
- Data processing - i.e., binary and string manipulation, data structures, file I/O, base64 decoding
- Discover and track information that cannot be found with ordinary plugins (PRMs)
- Knowledgebase building and database lookups
- Updated as part of the plugin feed - new functionality added regularly

Sample PASL application:

- NETBIOS detection - extract computer names
- Web agent enumeration - track web browsers being used by a host
- CPE reporting - look up CPE for an application/OS
- ViewState detection - Microsoft .NET passing web session state in an insecure manner
- ActiveX component detection on a web service - extract CLSID, look it up in table and report detailed associated vulnerability
- Default credentials detection - consult database of default credentials for services
- Account monitoring: POP3, MSN, IMAP, SMTP, AIM, Yahoo, Gmail
- Track DNS queries: client lookups, failed lookups, server name resolution
- File and data monitoring: FTP sites, SMB shares, NFS shares, log commands from client to server, maintain list of files being hosted on/downloaded from a server

Misc/Enhancements

- Added real-time logging of interactive and encrypted sessions
- Added PASL logging of performance and usage statistics to the pasl.log file located in the logs directory. Additional runtime information such as error messages are written to the pasl_scripts.log file.

Passive Vulnerability Scanner 3.4.0 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in PVS version 3.4.0, the significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

General Notes

As with any application, it is always advisable to perform a backup of the installation before upgrading.

Supported Platforms

Support is available for Red Hat ES 4, ES 5 and CentOS 5 64-bit.

Upgrading from 3.2.x

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
pvs-3.4.0-es4.i386.rpm	e2d348b708c2efeb59129dd85c783395
pvs-3.4.0-es5.i386.rpm	c748adda6fe52af06c70dcae91de92e5
pvs-3.4.0-es5.x86_64.rpm	6a8bf20e5d5f67a82c1c28a6d8d04d96
PVS-3.4.0-Dragon-skw.i386.tgz	0bd34aa2e5518f042cd15acb45945ea3

Application Notes

New Features

- New "exploitability" features for PVS. To maintain consistency with Nessus, PVS also provides new tags in vulnerability reports including: "core", "metasploit", "canvas" and "cvsstemporal" fields
- Added PVS watchdog capability to PVS Proxy

Misc/Enhancements

- Port scan detection has been removed as part of PVS 3.4's performance enhancements
- Replace GNU POSIX EREG API with PCRE API
- Replaced socket select with active packet wait
- Reworked encryption detection mechanism
- Replaced PVS packet filtering with BPF

Passive Vulnerability Scanner 3.6.0 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Windows - 11/15/2011, Linux - 1/23/2012

> **Note:** PVS 3.6.0.1 (Linux - 3/14/2012, Windows - 4/10/2012) fixes a wide variety of sensor stability and performance issues that were reported by customers shortly after the release of 3.6. 3.6.0.1 was extensively tested on customer networks and at this time resolves all stability issues Tenable is aware of.

The following list describes many of the changes that are included in PVS version 3.6.0, the significant issues that have been resolved, and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 4
- Red Hat Linux ES 5 / CentOS 5
- Red Hat Linux ES 5 / CentOS 5 64-bit
- Red Hat Linux ES 6 / CentOS 6
- Red Hat Linux ES 6 / CentOS 6 64-bit
- Windows Vista
- Windows Server 2008
- Windows 7

Upgrading from Windows 3.0.x

PVS 3.6 represents a significant upgrade from the previous Windows version. With a new UI for configuration and no real-time event GUI for monitoring events, the current version focuses on more seamless and efficient integration with SecurityCenter. As such, Tenable strongly recommends uninstalling any previous version and performing a fresh installation of PVS 3.6. A new license must be requested from Tenable Support. Licenses acquired prior to PVS 3.6 are not compatible with newer versions of the software.

File Names & MD5 Checksums

File	MD5
pvs-3.6.0.1-es4.i386.rpm	770639082eeb9d95e145861c0c3a8f37
pvs-3.6.0.1-es5.i386.rpm	e92431f073cc45ab6e5e4f41430d4e63
pvs-3.6.0.1-es5.x86_64.rpm	83d554b4323e7e6defb71294421d6549
pvs-3.6.0.1-es6.i386.rpm	64d488edba21ca74ede730f7b3895ff1
pvs-3.6.0.1-es6.x86_64.rpm	828577f3d16e1e8629e489169d11c9ea
pvs-3.6.0.1-i386.exe	0c1f682cef766fcde40163ae11e39333
pvs-3.6.0.1-x64.exe	1b41b48abe4057eff15112909fa18aef

Application Notes

- New graphical configuration editor for Windows version
- Added the "Strip VLAN tags" setting to ignore the VLAN header
- Added Nessus V2 report output format
- Deprecated the "failure-threshold" configuration setting
- Improved stability when parsing PASL scripts
- New license format ***Requires a new license**

This release is targeted for PVS implementations that are integrated with SecurityCenter and does not have a real-time UI component for browsing reported data. Future versions may provide this ability.

Passive Vulnerability Scanner 3.8.0 Release Notes - 12/4/2012

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in PVS 3.8, as well as significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running PVS 3.6.0 and later. Users upgrading from an older version must first perform an upgrade to PVS 3.6 before attempting to install version 3.8 or uninstall the previous version and performing a fresh installation of PVS 3.8.

PVS 3.8.0 is compatibile with existing versions of SecurityCenter 4.x and the new SC 4.6 release, however for integration with SC 4.6 you must ensure that the nessus-report format is enabled in the pvs.conf file.

Stop the PVS daemon before performing the upgrade:

```
# /etc/init.d/pvs stop
```

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

Supported Platforms

Support is available for the following platforms:

- Red Hat Linux ES 5 / CentOS 5 32/64-bit
- Red Hat Linux ES 6 / CentOS 6 32/64-bit
- Windows Server 2008 32/64-bit
- Windows 7 32/64-bit

The Microsoft Visual C++ Redistributable package is a prerequisite which needs to be installed on Windows before installing PVS. Refer to the documentation for more information.

File Names & MD5 Checksums

File	MD5
pvs-3.8.0-es5.i386.rpm	[ab12a98e4184265ba8d30e6bf2237c02]

File	MD5
pvs-3.8.0-es5.x86_64.rpm	[68e857119975c65220fe3d2fcc161497]
pvs-3.8.0-es6.i386.rpm	[b9f0f9eade4aa6d7546442959a39c2cd]
pvs-3.8.0-es6.x86_64.rpm	[d45e644c263f372e748badd21625117c]
pvs-3.8.0-i386.exe	[b0cb778b4b124a64b8463ef604695b31]
pvs-3.8.0-x64.exe	[92755934093f517fe3c636c5e04ab833]

Changes and New Features

New Features

- PVS now provides the ability to monitor IPv6 traffic including:
  - Real-time host or asset discovery
  - Detection of both encrypted and interactive sessions
  - Monitoring of traffic located within a 6to4 tunnel

  Note: When sending both IPv4 and IPv6 vulnerability data to SecurityCenter, both an IPv4 and IPv6 repository must be selected in the PVS sensor configuration.
- IPv6 addresses are supported in the configuration of include/exclude filters and for syslog destinations
- Added support for monitoring both VLAN & non-VLAN traffic simultaneously. Using a "VLAN" prefix for network inclusion VLAN networks can now be declared in the "monitored" and "excluded" networks section of the config file with the following syntax:
  vlan network/subnet;
- New plugin for Server Connections (ID 15); Similar to "show connections" but identifies the clients a "server" has established trusted relationships with
- Supports a user-defined port number for syslog destinations instead of just the default

Additional Improvements

- Reduced the default report-lifetime value to 7 days from 30. This is more closely inline with the default value used by SecurityCenter. If upgrading from a prior PVS version, it is recommended to manually change this value to 7.

- Improved real-time logging performance
- Tightened the file permissions of configuration files on Windows installations
- Added support for additional Nessus plugin tags. These will be included in the plugin feed in the near future.

Bug Fixes

- Addressed an issue that prevented the aging out of Knowledgebase Entries
- Addressed an issue with the transfer of large reports from PVS Proxy to SecurityCenter

Removed Functionality

- Removed the ability to generate XML and HTML reports
- Removed the "strip-vlan-tags" option in the config file in lieu of the new VLAN filtering syntax described above

Known Limitations

- Does not support IPv6 connectivity for the management connection from SecurityCenter (pvs proxy)
- There is no support for Teredo tunnels or IPv6 Extension Headers

Tenable OT Security Release Notes

To view EOL OT Security release notes, see Tenable EOL Release Notes.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

View the following OT Security (formerly Tenable.ot) release notes:

Tenable OT Security 2021

OT Security 2020

Tenable OT Security 3.15.42 SP (2023-04-24)

OT Security recommends that you upgrade to this version if you use split port configuration or active queries via sensors.

Bug Fixes

OT Security 3.15.42 SP includes the following bug fixes:

Bug fix
Nessus Scan via Sensor — Nessus Active Query can now send traffic via sensor route.
Nessus Scan in Split Port — Nessus scan can now work in split port mode (SFDC #01566712).
LDAP Settings — Resolved an issue in the user interface when creating a new LDAP Authentication Server (Local Settings > Users & Roles > Auth Servers > LDAP).

Tenable OT Security 3.15.39 SP (2023-02-24)

Note: Version 3.15.39 SP replaces the deprecated version 3.15.38.

New Features

New Vendor Support

- Basic passive and active support for Phoenix Contact - OT Security now passively and actively identifies the device model, family, type, and firmware version of Phoenix Contact (PCWorx and ProConOS protocols). This support also facilitates the detection of their vulnerabilities.

- Basic passive and active support for Profinet CM (Context Manager) - OT Security now passively and actively identifies the device firmware version, hardware version, order number, and type.

- Snapshot for Rockwell ControlLogix L8X and CompactLogix 538X families - OT Security can now take a snapshot for Rockwell controllers that are part of the L8X and 538X families.

- Ability to merge Siemens S7-300 and S7-400 with FW 2.6.7 and older - This feature is disabled by default and can be enabled only from the API.

- Enhancements for S7+ querying mechanism.

New Vulnerabilities (Plugins)

OT Security now identifies the new following vulnerabilities:

Vendor	Family/Model	Plugin ID
Siemens	Scalance	500788-500789, 500786, 500781-500783, 500778, 500772-500773, 500768, 500766, 500764, 500762, 500755-500760, 500749-500753, 500746, 500740-500742, 500735-500738, 500729
Siemens	Desigo	500787, 500785, 500779, 500776-500777, 500774, 500771, 500769, 500767, 500761, 500747, 500743-500745, 500735, 500730-500731
Siemens	Apogee	500748
Phoenix Contact	ILC, RFC, AXC, S_MAX	500784, 500780, 500775, 500770, 500765, 500763, 500754, 500739, 500732-500733, 500728

User-defined Nessus Scans

Nessus scans are now available through a dedicated page, allowing the user management, visibility, and flexibility in their scans:

- Management - You can now create, edit, delete, save, and run custom Nessus scans.

- Visibility - All plugins are visible and available for your selection.

- Flexibility - You can now choose to scan multiple network assets (endpoint type is excluded) through an IP range.

> **Note**: In case the IP range includes hosts that the system does not recognize as "network assets", OT Security does **not** scan those hosts.

IDS Engine Ruleset Updates

New IDS ruleset feed is available in OT Security. You can now obtain the newest set of IDS rules and install them at any time in two ways:

- Cloud update — For systems that are connected to the internet, IDS rules are periodically and automatically downloaded. You can also initiate this update on demand.
- Offline update — You can also upload a file containing the IDS rules to the system via the user interface. You can obtain the URL for this file from OT Security.

Dark Mode

Dark mode is now available in OT Security. It allows you to switch the color scheme of OT Security to a darker theme to provide a more comfortable viewing experience in low-light environments and potentially save battery life on your devices.

To activate dark mode, simply toggle the dark mode option on the top bar.

Export Dashboards

You can now export the dashboards on demand to a PDF file. If you export the dashboard when the dark mode is enabled, OT Security also generates the exported files in the dark mode format.

New Authentication Servers Page

You can now configure and manage your authentication servers' settings on the new Authentication Servers page (under the Local Settings - Users and Roles section).

On this page, you can now define, save, and enable multiple servers based on the authentication methods you use in your organization: Active Directory and LDAP.

Once configured, you can select the authentication server to which you want to connect in the login page's new drop-down menu.

Open Ports Mechanism Enhancements

The Open Ports table in the single asset page now shows all ports that were identified to be open. These include the current active port scans and passive conversations, active queries, Tenable Nessus, and Tenable Network Monitor.

You can control the desired aged-out period for considering a port to be open (under the Device page in the Local Settings - System Configuration section).

Usage Statistics

OT Security now gathers UI data for the purpose of learning, improving, and better understanding users needs.

When enabled (by default), Tenable collects telemetry information that cannot be attributed to a specific individual; it is only collected at the company level.

This information does not include Personal Data or personally identifiable information (PII). This can be turned on/off on the Device page under Local Settings - System Configuration.

Sensor - BPF from the Cockpit UI

Sensor BPF is now visible and available from the Cockpit UI.

Sensor - New Dedicated Port for the Authenticated Sensor

The sensor now uses a dedicated port (28304) for the authenticated sensor instead of the SSH port (22) that was used in V3.14.

The unauthenticated sensors remain in port 28303.

ICP V3.15 is now listening to both 22 and 28304 ports.

New Asset Types

OT Security now identifies the following new device types:

Category	New Type
Controller	BMS Controller
Controller	Backplane Module
Controller	Robot
Server	Security Appliance

Server	Tenable EM
Server	Tenable ICP
Server	Tenable Sensor

HTTP/HTTPS Banner Grabbing Enhancements

As of version 3.15, OT Security added several enhancements for HTTP/HTTPS banner grabbing such as querying more port numbers from which to collect banners, parsing HTTPS certificates, and more.

Compressed Backup File

You can now download a compressed system backup file from the Local Settings - System Actions page.

Custom Range Filter for IP Addresses

You can now filter the Inventory table for a specific range of assets based on a specific range of IP addresses.

EM - System Log

You can now view the Enterprise Manager (EM) System Log under the Local Settings menu.

EM - Factory Reset

On the Enterprise Manager (EM) you (the administrator) can now perform a factory reset on the machine and return it to its initial and default configuration.

API Changelog

For more information about the API, see the OT Security API documentation.

API breaking changes (removal of ServiceNow):

```
Enum value ServiceNow was removed from enum ActionType
Member ServiceNowServer was removed from Union type ActionUnion
Field serviceNowServers was removed from object type Integration
Field archiveServiceNowServer was removed from object type Mutation
Argument servicenowActions: [ID!] was removed from field Mutation.editPolicies
Field newServiceNowServer was removed from object type Mutation
Field setServiceNowServer was removed from object type Mutation
Field testAdHocServiceNowServer was removed from object type Mutation
Field testServiceNowServer was removed from object type Mutation
Field serviceNowServer was removed from object type Query
Field serviceNowServers was removed from object type Query
Type ServiceNowServer was removed
Type ServiceNowServerConnection was removed
Type ServiceNowServerEdge was removed
```

API additions:

```
Enum value extendedRunStatus was added to enum AssetField
Enum values BackplaneModule, Bms, Robot, TenableEm, TenableIcp, TenableSensor were added to enum
AssetType
Enum values InvalidFile, Unchanged were added to enum CannotUpdatePluginSetReason Enum values
NessusUserScan, ReadUpdates, WriteUpdates were added to enum Capability Enum value extendedRunStatus
was added to enum LinkField
Enum value PHOENIX_CONTACT, PROFINET_CM were added to enum ProtocolSuperType
Enum value PC_WORX, PROCONOS, PROFINET_CM were added to enum ProtocolType
Enum values BackplaneModule, Bms, Robot, TenableEm, TenableIcp, TenableSensor were added to enum
UserDefinedAssetType
Input fields bindDn, bindPw, domainAppend, groupBaseDn, host, port, userBaseDn were added to input
object type ProviderOptionsParams
Field APIKey.groups has description this property is always empty
Field APIKey.groups is deprecated
Field APIKey.groups has deprecation reason deprecated since 3.10 (RBAC), groups are determined by the
attached User
Field AdProviderOptions.rootCa changed type from String to String!
Field extendedRunStatus was added to object type Asset
Field compressionInProgress was added to object type BackupDetails
Fields lastModifiedBy, lastModifiedDate were added to objects ActivityPolicy, AssetGroup,
AssetFunction, AssetList, AssetPolicy, AssetTypeFamilyGroup, EmailGroup, IDSGeneralPolicy,
IDSSrcDstPolicy, IntrusionPolicy, IpList, IpRange, NetworkPolicy, Policy, PortGroup, PortPolicy,
ProtocolGroup, RecurringGroup, RuleGroup, ScheduleFunction, ScheduleGroup, SegmentGroup, TagGroup,
TagValuePolicy, TimeInterval
Type CanUpdateSuricataRuleSet was added
Enum value CannotUpdatePluginSetReason.PluginSetUnchanged was deprecated with reason this value will
change in the future to Unchanged, so always check for both
Type CannotUpdateSuricataRulesReason was added
Field backupCompression was added to object type FlagList
Type LdapProviderOptions was added
Type LdapProviderOptionsConnection was added
Type LdapProviderOptionsEdge was added
Field extendedRunStatus was added to object type LeanAsset
Field deleteNessusUserScan was added to object type Mutation
Field editNessusUserScan was added to object type Mutation
Field nessusUserScanAction was added to object type Mutation
Field newNessusUserScan was added to object type Mutation
Field updateSuricataRuleSet was added to object type Mutation
Type NessusUserScan was added
Type NessusUserScanConnection was added
Type NessusUserScanEdge was added
Field source was added to object type OpenPorts
Type OpenPortsSource was added
Field Plugin.id has description Plugin ID
Field Plugin.name has description Name
Field PluginDetails.cpe is deprecated
Field PluginDetails.cpe has deprecation reason please use cpes, this should be plural
Field cpes was added to object type PluginDetails
Field cves was added to object type PluginDetails
Type PluginFamily was added
Type PluginFamilyArgs was added
Type PluginFamilyConnection was added
Type PluginFamilyCount was added
Type PluginFamilyCountConnection was added
Type PluginFamilyCountEdge was added
Type PluginFamilyEdge was added
Type PluginsBasic was added
Type PluginsBasicConnection was added
Type PluginsBasicEdge was added
Type PluginsIndividualArgs was added
Type PluginsOfFamily was added
Field canOfflineUpdateSuricataRuleSet was added to object type Query
Field canOnlineUpdateSuricataRuleSet was added to object type Query
Field ldapAuthProviders was added to object type Query
Field nessusUserScan was added to object type Query
Field nessusUserScans was added to object type Query
Field pluginFamilies was added to object type Query
Field pluginsOfFamily was added to object type Query
Field suricataRuleSetDownloadUrl was added to object type Query
Field suricataRuleSetInfo was added to object type Query
Type ScanAction was added
Type SelectionStatus was added
Object type Subscription has description WARNING: Experimental feature! This can change without a
warning
Type SuricataRuleSetDownloadUrl was added
Type SuricataRuleSetInfo was added
Object type Time has description The `Time` scalar type represents date and time values as specified
by [RFC3339](https://www.rfc-editor.org/rfc/rfc3339.html).
Type UpdateResult was added
Type UserScanStatus was added
```

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are posted at OT Security Download page.

Tenable OT Security 3.14.25 (3.14 SP1) Release Notes (2022-09-20)

You can download the Tenable OT Security (OT Security) update files from the Tenable downloads page.

> **Note:** Starting with version 3.13, OT Security only supports Tenable Core. OT Security no longer supports Atomic OS. If you are unsure of what OS you have or how to upgrade to Tenable Core, contact Tenable support.

New Features

SAML Single Sign-On (SSO) Authentication

OT Security now support SAML (Security Assertion Markup Language) authentication to allow users of an IDP (Identity Provider, such as Azure AD) to use single sign-on to log in to OT Security.

Bug Fixes

OT Security 3.14.25 (3.14 SP1) includes the following bug fixes:

Bug fix
Version 3.14 ICP now supports Sensors version > 2.7.54 (the Sensor grid only lists versions > 3.7.18).
IEM Setup Wizard — The Network configuration step is now enabled again.
SC/IO Integrations — The SC/IO dashboards are now working again.
The selected items count is now correct in multi-selection grids.
Editing asset list applies now on all selected assets and not just the selected assets.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.14.xx

Product	Tested Versions
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.14.15 Release Notes (2022-08-08)

You can download the Tenable OT Security (OT Security) update files from the Tenable downloads page.

> **Note:** Starting with version 3.13, OT Security only supports Tenable Core. OT Security no longer supports Atomic OS. If you are unsure of what OS you have or how to upgrade to Tenable Core, contact Tenable support.

New Features

Usage Statistics

The Usage Statistics option specifies whether Tenable collects anonymous and non-sensitive telemetry data about your OT Security deployment. When enabled (by default), Tenable collects telemetry information that cannot be attributed to a specific individual; it is only collected at the company level. This information does not include Personal Data or personally identifiable information (PII). You can turn this option on or off on the Device page under Local Settings - System Configuration.

New sensor pairing and management

As of version 3.14, you can now use an authenticated sensor. The new sensor, based on Tenable Core OS, allows encrypted communication with the ICP through an SSH tunnel. You can also deploy the sensor on virtual machines. OT Security shows all sensors (version 3.7.18 and later) connected to the ICP on the new sensor page in the ICP as well as in a new widget on the inventory dashboard. The following new management options are available on the sensor page:

- Pause and resume data
- Delete and unpair sensor
- Edit sensor name
- Query actively more networks through the sensor

The option to connect the ICP to an unauthenticated sensor is still possible as in versions before 3.14. This option still appears in the grid with the following minimal management options:

- Edit sensor name
- Delete sensor

Active sensors

As part of the sensor's management options, you can now actively query assets accessible from the sensor. This significantly increases the sensor's capability to discover and identify assets.

You can manage the specific networks that each sensor should query. Once you define a network, the assets on that network become available for querying via the sensor's tunnel. Previously only the ICP could perform active queries, so some assets may not have had a networking route from the ICP.

You can manage this new capability centrally on the ICP for each authenticated sensor and for each specific network.

Notes:

- This feature does not support active queries over layer 2.
- You may encounter events associated with the sensor itself, which you can exclude if needed.
- This ICP version does not support sensors version 3.7.18 and earlier. This will be fixed in the next SP.

Data plane monitoring for ICCP / IEC 60870-6/TASE.2

OT Security now passively monitors ICCP, a data plane protocol based on MMS, and detects the following common commands:

- MMS Define Named Variable List
- MMS Delete Named Variable List
- ICCP Create Dataset
- ICCP Bilateral Table Exchange

Predefined policies for the ICCP commands are now available. You can now configure and define these policies to monitor such events.

Standard passive support for Bosch PSI Controllers

OT Security added standard passive support for Bosch PSI controllers to facilitate the detection of common commands:

- Bosch PSI Connect
- Bosch PSI Disconnect
- Bosch PSI Download Config
- Bosch PSI Reset

Predefined policies are now available. You can now configure and define these policies to monitor such events.

Basic passive support for Schneider ION Power Meters

OT Security now passively identifies the device model, family, type, and firmware version of ION power meters. This support also facilitates the detection of their vulnerabilities.

Basic passive support for Wago 750 Controllers

OT Security now passively identifies the device model, family, type, firmware version, hardware version, and the serial number of Wago 750 controllers. This support also facilitates the detection of their vulnerabilities.

Permanent deletion of assets (API)

You can now delete assets completely with the API using the assets' IP addresses or CIDRs. This deletion propagates throughout the system (Inventory tables, Network map, Events tables, Attack vectors, Groups, License).

> **Notes**:
>
> - When you delete an asset that is part of a backplane, OT Security also deletes the entire backplane.
> - If a deleted IP address reappears over the traffic, OT Security rediscovers the asset.

Localization

You can now change the language of the interface to French, German, Japanese, and Chinese.

UX/UI Improvements

- Redesign of the Device settings page.
- A new Port Configuration settings page - the port configuration section moved to a new dedicated page in the System Configuration settings.

New Tools

Idle Assets Hider Tool

The Idle Assets Hider Tool helps you keep your Inventory tables up-to-date. By using this tool, all assets that have been unavailable for a specified amount of time that you configure will be hidden.

Hidden Assets Deletion Tools

This tool allows you to delete hidden assets permanently. You can use this tool to delete assets quickly by first hiding the assets you want to delete and then running this tool.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.13.35.

Product	Tested Versions
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.13.36 Release Notes (2022-05-22)

You can download the Tenable OT Security (OT Security) update files from the Tenable downloads page.

> **Note:** Starting with version 3.13, OT Security only supports Tenable Core. OT Security no longer supports Atomic OS. If you are unsure of what OS you have or how to upgrade to Tenable Core, contact Tenable support.

New Features

Suricata Signatures for Detecting Triton attacks

OT Security added new Suricata signatures to flag exploitation attempts from the Triton attack.

Use of HTTP Proxy in OT Security (Tenable Vulnerability Management and Plugins updates)

OT Security now enables its services to access the internet using the proxy host configured in Tenable Core.

> **Note**: While it is possible to configure an HTTPS proxy in Tenable Core, it does not work.

Support of DIGEST Authentication Method for Banner Grabbing

OT Security now grabs banners that use the DIGEST authentication method.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.13.35.

Product	Tested Versions
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.13 Enterprise Manager Release Notes (2022-05-19)

You can download the Tenable OT Security (OT Security) update files from the Tenable downloads page.

> **Note**: Starting with v. 3.13, we only support Tenable Core. We no longer support Atomic OS. If you are unsure of what OS you are running or how to upgrade to Tenable Core, please contact Tenable support.

New Features

Enterprise Management Dashboards

OT Security now has a brand new dashboard that offers dozens of user-configurable widgets. These widgets display the aggregated information about assets, risks, and vulnerabilities from across all the connected sites and provide an enterprise-wide view.

The following are some examples of the metrics that the new dashboards address:

- Risk — For insights into the network's cyber exposure by looking into asset risk scores and vulnerability management metrics.
- Asset Inventory — For various summaries and breakdowns of the assets.
- Events and Policies — For the means to detect the various network threats.

Enterprise Management Setup Wizard

A GUI-based setup wizard for an easy and quick enterprise management configuration.

New Enterprise Management Integrations with Tenable Vulnerability Management and Tenable Security Center

The Enterprise Management now supports integrations with Tenable Vulnerability Management and Tenable Security Center. You can use it as a single and centralized integration point for multiple ICPs across multiple sites to Tenable Vulnerability Management and Tenable Security Center.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.13 Enterprise Manager.

Product	Tested Versions

Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.13.35 Release Notes (2022-05-19)

You can download the Tenable OT Security (OT Security) update files from the Tenable downloads page.

Caution: Version 3.13.35 is deprecated and replaced by version 3.13.36.

New Features

Suricata Signatures for Detecting Triton attacks

OT Security added new Suricata signatures to flag exploitation attempts from the Triton attack.

Use of HTTP Proxy in OT Security (Tenable Vulnerability Management and Plugins updates)

OT Security now enables its services to access the internet using the proxy host configured in Tenable Core.

Note: While it is possible to configure an HTTPS proxy in Tenable Core, it does not work.

Support of DIGEST Authentication Method for Banner Grabbing

OT Security now grabs banners that use the DIGEST authentication method.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.13.35.

Product	Tested Versions
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.13.21 Release Notes (2022-02-28)

You can download the Tenable OT Security (OT Security) update files from the Tenable downloads page.

Note: Starting with version 3.13, OT Security only supports Tenable Core. OT Security no longer supports Atomic OS. If you are unsure of what OS you have or how to upgrade to Tenable Core, contact Tenable support.

New Features

Migration to Plugins-based Vulnerabilities Detection

Starting with v. 3.13, OT Security bases vulnerabilities detection on plugins, as in all other Tenable products. Plugins are written in a proprietary scripting language, called Nessus Attack Scripting Language (NASL), and contain vulnerability information, a generic set of remediation actions and the algorithm to test for the presence of the security issue.

You can obtain the newest set of plugins and install them at any time in two ways:

- Cloud update - for systems that are connected to the internet, plugins are periodically and automatically downloaded. You can also initiate this update on demand.
- Offline update - You can also upload a file containing the plugins data to the system via the user interface. You can obtain the URL for this file from OT Security.

The migration to plugins will affect the risk score of assets.

To learn more about plugins, visit: https://docs.tenable.com/nessus/Content/AboutNessusPlugins.htm.

Event Clusters

OT Security groups into a cluster the events that were triggered by the same policy and that are adjacent in time and have identical characteristics. This reduces the number of records in the user interface and simplifies both initial policies tuning and incident response in case of an event.

Tools for Policies Tuning

OT Security calculates and presents the following data and for each policy:

- Number of generated events - you can now see this information for the last 24 hours or last 7 / 30 days.
- Number of created exclusions.

New Dashboard Widgets

OT Security added the following widgets in connection to the migration to plugins-based vulnerabilities detection:

- Most common vulnerabilities
- Most common plugin families
- Vulnerabilities by severity
- Most severe vulnerabilities

OT Security also added the following widget:

- Most common policies

Uploading Asset Data via the UI

You can now upload a CSV file with data of assets that do not exist in OT Security to leverage its asset management capabilities.

Detection of NUCLEUS:13 Exploitation Attempts

OT Security added Suricata signatures for flagging exploitation attempts of NUCLEUS:13 vulnerabilities.

Uploading an HTTPs Certificate via the UI

You can now upload an HTTPs certificate via the user interface, as opposed to only generating a self-signed certificate.

Bachmann M1 Standard Passive Support

OT Security added standard passive support for Bachmann M1 controllers to facilitate, among others, the detection of common code and controllers' state changes.

Localization

You can now change the user interface's language to both Japanese and Chinese.

Settings Redesign

OT Security redesigned the local settings section and the systems actions page to improve usability.

Downloading Diagnostics via the CLI

You can now download a diagnostics file via the command line interface (CLI) when the user interface is not accessible.

Deprecated Features

- Risk tab - due to migration to the plugins-based vulnerabilities detection, OT Security replaced both the CVEs and old vulnerabilities sub-tabs with a single new vulnerabilities tab.
- OT Security did not yet translate vulnerabilities whose origin is not a CVE to plugins, which means that you are temporarily unable to see them in v. 3.13, even if they were detected in earlier versions.
- The SNMP agent on OT Security is no longer available. You must use the SNMP Agent on Tenable core.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.13.21.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.12.26 (3.12 SP3) Release Notes (2022-01-12)

If you are running these OT Security versions or later, you can upgrade directly to version 3.12.26.

Bug Fixes

Tenable OT Security (OT Security) version 3.12.26 contains the following bug fixes:

Bug Fix
The Log4jShell scan no longer creates non-existent assets.
Upgrading a system with more than 30K files in the directory no longer causes the system to halt and fail the upgrade.
Upgrading system with a large database size no longer causes timeout in upgrade scripts.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.12.26.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 2021

- Tenable OT Security 3.12.24 (3.12 SP2 / Log4Shell) Release Notes (2021-12-21)
- Tenable OT Security 3.12.16 Release Notes (2021-11-18)
- Tenable OT Security 3.11.23 Release Notes (2021-09-03)
- Tenable OT Security 3.11.18 Release Notes (2021-06-24)
- Tenable OT Security 3.10.38 Release Notes (2021-05-13)
- Tenable OT Security 3.10.30 Release Notes (2021-04-02)
- Tenable OT Security 3.9.25 Release Notes (2021-02-18)
- Tenable OT Security 3.11.25 Release Notes (2021-10-28)

Tenable OT Security 3.12.24 (3.12 SP2 / Log4Shell) Release Notes (2021-12-21)

If you are running these OT Security versions or later, you can upgrade directly to version 3.12.24.

New Features

Tenable OT Security (OT Security) version 3.12.24 contains the following new features:

New Scan for Log4Shell Vulnerability Identification

OT Security allows you to perform a scan of your inventory to identify vulnerable devices related to the recently disclosed Apache Log4jShell vulnerability (CVE-2021-44228). OT Security based this feature on the Nessus plugins which became available to address this vulnerability.

You can launch this scan manually and have full control over which assets to scan.

New Suricata Signatures to Detect Log4Shell Vulnerability

The new signatures allow OT Security to flag exploration attempts on the Log4Shell vulnerability.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.12.24.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.12.16 Release Notes (2021-11-18)

If you are running these OT Security versions or later, you can upgrade directly to version 3.12.16.

New Features

Tenable OT Security (OT Security) version 3.12.16 contains the following new features:

Dashboard

OT Security now has a brand new dashboard that offers dozens of user-configurable widgets. Some examples of the metrics it addresses are:

- Risk — Providing insights to the network's cyber exposure by looking into the asset risk score and vulnerability management metrics.
- Asset Inventory — Providing various summaries and breakdowns of the assets.
- Events and Policies — Providing the means to detect the most varied network threats.

S7-300/400 Backplane Scan Improvements

OT Security now identifies all the backplane modules of an S7-300/400 controller (in addition to the CP and CPU detected so far), in particular when the hardware configuration comes from TIA-portal.

Verbose Active Queries Error Handling

Manual error notifications of active queries now include more details.

Support for Palo Alto Networks Firewall DAGs Based Integration for v9.1/v10

The OT Security integration with PAN's firewall now supports both NGW v9.1 and v10.

UX/UI Improvements

- Redesign of the snapshots page.
- Redesign of the constant nag message.
- New 'First Seen' column in the Inventory tables.

LDAP Based Login Improvements

There is no longer the need to type the domain name when logging in using LDAP-based authentication.

License Reinitialization

You can apply a new license code to OT Security to replace the current license without first having to delete the existing license.

Deprecated Features

- Risk Assessment Report

Bug Fixes

Bug Fix
The IEM Cluster upgrade works correctly.
OT Security works while you disable the active tracking query.
OT Security now supports direct upgrades from versions 3.9.25 and earlier.
OT Security now shows asset connections in the single asset page network map.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.11.23 Release Notes (2021-09-03)

If you are running version 3.9.25 or later, you can upgrade directly to version 3.11.23.

New Features

Refinement of Automated Asset Creation Heuristics

OT Security will not automatically create assets if their IP addresses are outside the monitored ranges.

Additional Suricata Signatures to Detect PwnedPiper Vulnerabilities

The signatures will flag exploitation attempts on PwnedPiper vulnerabilities.

Detection of Profibus Faults in Siemens Controllers

OT Security now detects these faults.

Bug Fixes

Bug Fix
OT Security no longer reports removed (hidden) assets to Tenable Security Center and Tenable Vulnerability Management.
OT Security no longer queries removed (hidden) assets.
OT Security will also report indirect IP addresses to Tenable Security Center.
OT Security will no longer stop working when parsing malformed DNS packets.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.11.18 Release Notes (2021-06-24)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

If you are upgrading Tenable Core + OT Security, follow this KB: https://tenable.my.salesforce.com/articles/How_To/Upgrade-Cobex-running-on-Tenable-Core.

New Features

Network Segmentation

OT Security now automatically assigns each asset to a default segment, based on its IP address and taking the asset type into account. The user can also manually adjust the segmentation for it to reflect the network topology in the best way possible.

Network segments can be used for policy configurations, similarly to asset groups.

Tenable Network Monitor Integration

The Tenable Network Monitor detection engine in now fully a part of OT Security, which adds various asset details extraction, classification and vulnerabilities detection capabilities.

IEM Changes

- IEM will now allow accessing up to 500 connected ICPs - showing assets, events, and vulnerabilities for each of them.
- IEM will no longer show the aggregated views of assets and events (this information will be gradually presented in Tenable Vulnerability Management).
- IEM users will be now presented with the status of connected ICPs, have access to the IEM's system settings.
- IEM can now support multiple users of the 'administrator' type.

SICAM A8000 - Standard Active Support

OT Security now actively extracts the device name, family, model, type, firmware version, hardware version, plant and region of SICAM A8000 RTUs.

Licensing - Aging Out IP Addresses

IP addresses can now be aged out after 30 days if they are not seen as active in connection to a specific interface. Once aged out, the IP address won't be counted against the licensed assets count.

API Freeze

The OT Security GraphQL based API is from now on the official publicly available external API.

Showing the Size of a Backup File

Users can now see the size of the created system backup file, in the system settings tab.

Bug Fixes

Bug Fix
SNMP V2 queries were not triggered as part of the SNMP queries if the SNMP V3 configuration was set.
The user was able to delete all monitored networks, causing the system not to start.
After migrating a non-Tenable Core system to a Tenable Core + OT Security system, DBs were fully deleted.
Eng station was appearing as part of S7 controller backplane.
DNS name of an asset that resided on a backplane affected all other backplane's assets' DNS names.
Upon completion of the setup wizard, redirection was done immediately to the login page, instead of the restarting page.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.10.38 Release Notes (2021-05-13)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Feature

Bulk Remove and Restore Assets

Users can now remove assets (and later restore them) in bulk, to ease these actions if they need to perform an action on many assets at once.

Bug Fixes

Bug Fix
Code revision (snapshots) page was not updating correctly
During installation not all PCAP folders were created
The machine was not starting when having a bond interface
Sending events when involved asset had a custom field fails
UDP timeout did not work for NETBIOS' active client

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.10.30 Release Notes (2021-04-02)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

Vendor Support

- Unitronics Vision - Standard Active Support
- Saia PCD - Standard Passive Support
- GE 90-30, RX3i, Rx7i, VersaMax - Standard Active Support
- Basic Active Support added for the following devices:
    - Yokogawa STARDOM
    - Omron CJ2
    - Eaton SMP Gateways
    - Cisco Stratix 5400
    - Brocade ICX 6610
    - Brickcom Network Cameras

OT Security Licensing

OT Security now uses the same licensing mechanism that the rest of the product suite is based on. The license type depends on the number of monitored assets and is subscription based.

> **Note:** Users upgrading from a version earlier than OT Security 3.10.x should make sure they have an activation code ahead of the upgrade to make sure the upgraded system is fully licensed.

Use a CSV Editor to Edit Asset Characteristics

Users can now use an external CSV editor (e.g. Microsoft Excel) to set or change the user-editable data fields of assets. To use this, export the All-Assets grid to a CSV file, edit (the editable) details and then upload the result file via the asset settings sub-tab.

Role Based Access Control

New roles and ways to manage groups of users were added. Four new types of roles —supervisor, security manager, security analyst and site manager— can now be assigned to every new user that is being created. Each of these user roles has its own designated permissions. The system also supports user groups that allow managing users that have the same role, together. These two new capabilities help make user and permissions management easier and more flexible.

Notes:

- API Keys - Starting in version 3.10, external users (Active Directory users and any other authenticated external users) won't be able to create API keys. This change was done since API keys are now directly attached to specific users, as opposed to roles. Existing API keys that were created using AD users will be migrated from the original AD user that created them to two new users that will be created automatically - "Migrated Admin API Key" and "Migrated Read-only API Key". Each one of these users will hold the relevant API keys. In order to login into these two users, the local admin will need to change their passwords. In addition, Read-only API Keys of local admin users will be migrated to the "Migrated Read-only API Key" user.
- Active Directory Admins (External Admins) will not be able to manage local users, change the AD settings or perform factory resets to the device.
- IEM users will no longer be able to manage local users, generate API keys or change the AD settings on local ICP devices.

Upgrading OT Security from the Tenable Core Interface

Users can now upgrade their product version via the Tenable Core operating system interface. While this feature is being introduced in version 3.10 it'll naturally only be used in practice when a SP of it or V.3.11 will be released. This greatly simplifies the system upgrade process, allowing users to be always up-to-date with the latest-and-greatest product capabilities as well as security related patches.

New Custom Field Type - Hyperlink

Users can now navigate directly from the user interface to remote network locations, by using a custom field of the new type 'hyperlink,' purposed for web addresses or remote network data folders.

FortiGate Integration

The integration with FortiGate allows using OT Security events to automatically create firewall rules (known as 'enforcement policies' in FortiGate) of FortiGate's next-generation firewalls in order to block unwanted or malicious communications

Detailed Event Emails

The emails users receive as a result of an event will now include more comprehensive information about it, including the policy that triggered the event and data regarding the associated assets.

Bug Fixes

Bug Fix
Active Directory | Configurations | user selected certificate not send by user interface
Grids | BE Filters | UI failed to open filter options and start infinite loop
Edit rule group | edit a group when all available rules are selected is causing to page unresponsive

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.9.25 Release Notes (2021-02-18)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

Vendor Support - Bachmann Secure Configuration Active Support

OT Security now supports password protected Bachmann PLCs. This way users can protect their controllers with passwords, and also leverage OT Security Active Query capabilities to monitor their PLCs.

Basic Active Support

OT Security constantly increases coverage of detection of OT/IoT devices based on research. In this release we added Basic Active Support for the following devices, and more:

- Sofrel Lacroix
- Illustra Cameras
- Netgear Switches
- Sierra Wireless AirLink Access Points

Additional Intrusion Detection Rules of Recent Campaigns

In addition to the regular update of our signatures database with the latest Suricata signatures available publicly, we highlighted two sets of signatures as purpose-built groups (rule groups):

- Rules released by FireEye to identify the use of Red Team tools that were stolen from them through a cyber attack, as described in a FireEye blog post.
- Rules to identify the SolarWinds Orion attack based on the Sunburst malware, as made public by FireEye.

Bug Fixes

Bug Fix
Setup wizard won't load
Incorrect SID displayed in email report
WMI query fails on non-English machines
Pre-auth download links don't work on IEM (returns 401 unauthorized)
Event pcap not using self sniffing pcaps
Migration from some machines that were previously upgraded from 2.7 failed

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

Tenable OT Security 3.11.25 Release Notes (2021-10-28)

Bug Fixes

Bug Fix
Tenable OT Security (OT Security) now supports upgrades from versions prior to 3.9.25.
The network map for a single asset in the single asset page now displays a link.
OT Security now tracks active assets 10x faster.

API

For more information about APIs for this release, see the OT Security API Guide.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

OT Security 2020

OT Security 2020

OT Security 3.4.25 Release Notes (2020-03-18)

OT Security 3.4.26 Release Notes (2020-03-27)

OT Security 3.4.9 Release Notes (2020-02-01)

OT Security 3.5.13 Release Notes (2020-04-08)

OT Security 3.5.29 Release Notes (2020-05-07)

OT Security 3.6.26 Release Notes (2020-06-17)

OT Security 3.6.33 Release Notes (2020-07-14)

- OT Security 3.7.18 Release Notes (2020-08-10)
- OT Security 3.7.22 Release Notes (2020-09-14)
- OT Security 3.8.13 Release Notes (2020-10-08)
- OT Security 3.8.15 Release Notes (2020-10-16)
- OT Security 3.8.17 Release Notes (2020-11-09)
- OT Security 3.9.14 Release Notes (2020-12-15)

OT Security 2020

OT Security 3.4.25 Release Notes (2020-03-18)

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

PCAP Simulation via API

OT Security enables users to leverage the API in order to simulate traffic from PCAP files. Users can play any one of the following formats: `pcap`, `pcap.gz`, `pcapng`, `pcapng.gz`.

For more information on how to use the API, see the knowledge base article (requires an account).

Bug Fixes

Bug Fix
General
Tenable Security Center import tool failed to import data for asset missing IP address array.
Performance
Proxy Arp Auto Detection Fix.
Improved Queue Management & Draining.
Fixed Services Startup Issues.

Improved Efficiency in DB Transactions.
User Interface
Fix Log In Flow Issue.
Fix Event Severity Filter Missing Values.
Fix "Resync" Behaviour.
Fix Report Configuration Not Working.
Missing the show password option in "Retype New Password" field
Change in Navigation Tree to include Reports in Main Navigation.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.4.25.

Product	Tested Version(s)
Tenable Security Center	5.11 and later

OT Security 3.4.26 Release Notes (2020-03-27)

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Bug Fixes

Bug Fix
Fix Asset Map Expired License Watermark
Fix Install Process with a large number of pcaps
Fix ABEthernet PCCC Issues
Fix Risk Score Calculation Timeout
Fix DB Upgrade Race Issue
Fix ABethernet shepherd infinite loop

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.4.26.

Product	Tested Version(s)
Tenable Security Center	5.11 and later

OT Security 3.4.9 Release Notes (2020-02-01)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

New OT Devices Support

Support for the following models was added:

- Yokogawa Prosafe - Level 1 Passive Support
- Honeywell C300 - Level 1 Passive Support
- PLC5 - Level 2 Passive Support, Level 2 Active Support
- Serial DH+ Connection - Level 2 Passive Support, Level 2 Active Support
- Cognex In-Sight Cameras - Level 1 Passive Support, Level 2 Active Support

The full list of vendor support and support levels description can be obtained from a sales engineer representative.

New SCADA Protocols Support

- Detection of Modbus error codes – three new Modbus error codes are now flagged using designated policies - ‘illegal data address’, ‘illegal data value’ and ‘illegal function’.
- Detection of IEC 60870-5-104 commands - several risky commands in IEC-60870-5-104 are now flagged using designated policies. Some examples for those are: Start, Stop, Reset and Data Transfer.

Asset Criticality

An OT Asset Risk Criticality was introduced (Low / Medium / High). The predefined value is based on the asset type, but it can be altered by the user. A 'none' level is also supported.

Asset Risk Score

An OT Asset Risk Score was introduced (ranging between 0 and 100). It is being calculated based on the events, vulnerabilities and CVEs associated with the asset and its criticality.

Integration with Tenable Security Center

The integration of OT Security and Tenable Security Center utilizes OT CVE data to facilitate a unified VM platform across IT and OT. For configuration information, see the knowledge base article (requires an account).

Detection of Network Traffic & Conversations Spikes

The user can now receive alerts on anomalous network traffic throughput as well as an anomalous number of conversations taking place. Both metrics are often associated with the existence of an infected or a malfunctioning device/s. The referenceable time window and the sensitivity level to changes in the traffic are user configurable via the relevant policy.

USB Configuration Changes

The user can receive alerts on changes in the list of USB devices connected to MS-Windows machines, thus identifying insertion or removal of these devices. The frequency of this query is defined separately from the other WMI queries to enable more frequent settings.

Switch Interface Details

Mapping of all the interfaces of network switches is done periodically to monitor their state and health, including MAC addresses, name, status, alias, description and type for each interface. For configuration help, contact your Tenable representative and see the knowledge base article (requires an account).

Report Configuration

When generating a report, users can now control the asset drill-down portion. They can either exclude it completely or have it for only certain asset types, per their preference.

Health Check API

An API to query the system for its health state was introduced at:

GET https://<IP>/v1/healthcheck. It contains details regarding the hardware health, container health, the connected sensors throughput and other details.

New API authentication Method

Authentication using tokens was introduced in addition to the use of robots. The new method allows for authentication using an HTTPS authorization header:

```
"Authorization: Key <API token>"
```

or a URL parameter: https://IP/v1/<API request>?apikey=<API token>

System Log Export

System log messages can now also be sent over Syslog to SIEM products.

Deprecated Features

Change
Alerts drill down chapter in the report - The Alerts Drill Down chapter has been removed from the report. Indegy v3.4 has events instead of alerts, and hence this chapter is deprecated.
Showing the diagnostic buffer of Siemens Controllers - This query is no longer supported by the core platform and is removed from the UI.

Bug Fixes

Bug Fix
Resolve All Events Not Working
Policies Search and Filter Not Persistent on Reload
Asset Editing Requires Hard Refresh to Apply Values
Vulnerability Matching Overmatching in Some Cases due to NVD formatting

OT Security 3.5.13 Release Notes (2020-04-08)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

New OT Devices Support

- SICAM AX - Standard Active Support
- Siprotec 4 - Premium Active Support
- Concept - Premium Active Support
- Beckhoff - Basic Passive & Standard Active

PCAP Extraction for Events

Event-specific capture files (in .pcap format) are now available for users to download and investigate on third party platform, or for sharing with non-users of OT Security. Selected as a row action, a .pcap file is generated and downloaded, containing only event-related traffic.

Terminology Update - Vulnerabilities & CVEs

Updated terminology when describing vulnerabilities in order to align with other Tenable products. In previous releases, the term "vulnerabilities" was used to described CVEs (Common Vulnerabilities and Exposures) – now, the term will be CVEs.

Remove Assets

Users can now remove assets from OT Security solution. Remove assets is available from the Single Asset Page via the Inventory Grid Action. Removed Assets can be viewed and restored from the Settings > Assets > Removed Assets page.

Asset Discovery "Run Now"

The Asset Discovery Query, aimed to discover assets periodically, can now be initiated on demand. This query can be configured and initiated from Settings > Queries > Asset Discovery.

Set-up Wizard for OT Security Sensors

OT Security sensors are utilized to collect traffic from remote network segments that are not visible from the main switch. The new Sensor Set-up Wizard enables users to define the IP of the Sensor as well as the IP of the OT Security platform to which the sensor will be sending the compressed data from the remote network.

Bug Fixes

Bug Fix
Fix issue with Setup Wizard Finishing
Set Date is set for one day before user selection
Fix user defined Asset Types do not affect asset risk score
Fix No Results in Grid Filters
Update Asset Map License - Remove Watermark
Fix report hanging with configuration
Fix missing asset details in specific policy scenario
Fix Resync button clickability

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.5.13.

Product	Tested Version(s)
Tenable Security Center	5.11 and later

OT Security 3.5.29 Release Notes (2020-05-07)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features

Vendor Support

- Siemens S7-1200 & S7-1500 - Premium Active Support
- Niagara AX & Niagara 4 - Standard Active Support
- Basic Active Support for Multiple OT/IOT Devices - Schneider Electric PowerLogic, Bosch IndraControl, Siemens Scalance, Siemens RS900, Moxa EDS, Moxa NPort, Moxa MGate, Cisco Stratix 5700, Cisco Catalyst, Cisco IE-2000, Cisco IE-5000, Lantronix and others.

Improved IEM Upgrade Process

Simplifying IEM Cluster Upgrade by automating the process from the IEM based on SSH connection between IEM and IMS.

For more information, see the knowledge base article (requires an account).

Bug Fixes

Bug Fix
Report Performance Improvements
IEM Redirect Bugs on Specific Site Pages
IEM Site Name Consistency
SIPROTEC 5 FW Change Event Issues
Post Upgrade Some Grids State Returns to Default
S7-1200 Firmware Changes False Positives due to Invalid Packets

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.5.29.

Product	Tested Version(s)
Tenable Security Center	5.11 and later

OT Security 3.6.26 Release Notes (2020-06-17)

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

For documentation relating to this release, see the OT Security 3.6.x User Guide.

New Features

Vendor Support

- Bachmann M1 - Standard Active Support
- Moxa Devices - Basic Passive Support

Threat Detection

- DNP3 Events - The system now detects various DNP3 commands, e.g. Select, Operate, Warm/Cold restart etc, as well as errors originating from internal indicators, such as function codes that are not supported and parameter related errors.
- Non-secure FTP and Telnet logins - The system now alerts on login attempts in both FTP and Telnet, and indicates whether the login was successful or not.
- ABB Data Plane events - The system now detects unauthorized MMS write events to ABB 800xA controllers. With that, users can get alerts on any write commands, and set allowed ranges for operational parameters. This is currently available only over the API.

Risk Widget

A designated widget presenting the risk score of each asset was added. This widget consists of a breakdown of the different components on which the risk score of the asset is based - e.g. the events associated with it, its detected vulnerabilities as well as its user defined criticality.

Vulnerabilities

The system now detects various asset-specific and network-wide vulnerabilities, beyond CVEs. Examples are: existence of obsolete versions of M-S Windows, usage of unsafe protocols and open network ports known to be risky.

Exclusions

The system now allows the user to exclude an event from a policy. Excluding an event after it was flagged will mean there'll be no future occurrences of similar events as a result of the same policy. This increases the user control over which events are being flagged and reduces false positives. This is being done directly from the events grid.

Usability Improvements

- Bulk Edit of Asset Details - Users can now edit details of multiple assets at once. Users can select a range of assets using Shift Key.
- Expansion of the Events Power Panel - Users can now set the height of the Power Panel in the Events grid -either collapsing it to ease browsing through the grid or expand it to investigate the details of a certain event.
- The system now allows users to configure the accessible URL for the UI (FQDN), supporting only one accessible URL at any given time.

Berkeley Packet Filter

Berkeley Packet Filter (BPF) was now implemented on the ICP, to allow filtering inbound traffic to it.

Bug Fixes

Bug Fix
Groups name links are not working.
Reports - "Failed to generate report" is displayed, but report is created.
Vulnerabilities single page - Actions button is disabled.
Policies - SCADA Events - Can't create DNP policies.
Read only user - Vulnerabilities - Single page is not displayed.
FTP Events - Event trigger without details - Should extract the clear text credentials.
Events - Download capture file - Can't download pcap for event when first capture file is still ongoing.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with OT Security 3.6.26.

Product	Tested Version(s)
Tenable Security Center	5.11 and later

OT Security 3.6.33 Release Notes (2020-07-14)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

To download OT Security upgrade files, see: https://tenable-ot.sharefile.com/d-s8ba6342ec004b86a.

For a list of previous versions that are possible to perform a direct upgrade from, see: https://tenable-ot.sharefile.com/d-s10cc31311564736a.

New Features

Vendor Support

- Premium Support for ABB RTU 540/560

Tenable Vulnerability Management Integration

- Added integration capabilities to Tenable Vulnerability Management. Integration setup is done with Tenable Support assistance and requires a Tenable Vulnerability Management Access Key, and Secret Key.

Detection of Ripple20 exploit attempts

- Added an Intrusion Detection rule group which will detect successful identification attempts or exploits of Ripple20 affected assets over the network.

API

- API Key - API improved to align with the standard Rest API spec. Starting 3.6.33, the API uses the 'X-APIKey' header instead of 'Authorization'

  The new header is: 'X-APIKeys: key= <API_KEY>'

  For example:

  ```
  curl -v -k -H 'X-APIKeys: key=Mbvf2sXdROWBrB99MBXwXN-
  LqYrWVxPEyos1IJk9e9aNPLOlWalkHkAfsS4=' https://IP/v1/status
  ```

Bug Fixes

Bug Fix
Grouping Assets by Site fix for Enterprise Manager
Appliance Data Auto-Refresh for Enterprise Manager
Network Summary Widgets Fix of Units & Colors
Traffic and conversation graph on Network Traffic Summary fixed
Filter for empty missing name "Blank" in Exclude from policy

Fix Siprotec4 snapshots conversation delay check
Fix empty data in single vulnerability page
Active Querying RTU 540 failed
Missing the show password option in "Retype New Password" field
Fix save button is enabled when it should not for bulk edit assets
Setup wizard | Split Interface | Fields name are not displayed until clicking on the screen/refresh
Conversation | Duration column filter is not sorted correctly
User unable to copy data from UI
Additional Suricata rules to 3.6 SP
Unicode decoding issue for WMI querying for USB details
ABB RTU 540/560 Premium Support

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later

OT Security 3.7.18 Release Notes (2020-08-10)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

To download OT Security upgrade files, see: https://tenable-ot.sharefile.com/d-sfde665c7b9942aba.

For a list of previous versions that are possible to perform a direct upgrade from, see: https://tenable-ot.sharefile.com/d-sb0d4e3b0df840318.

New Features

Vendor Support

- Emerson Ovation - Standard Active Support
- Siemens S7+ - Premium Support Including Full Backplane Inventory
- HART Protocol - Basic Passive Support

Asset Types - Increasing Type Catalog

OT Security has taken another step forward to diversify the available types for asset classification. With that, it can better communicate to its users granular findings on their inventory and increase familiarization. On top of that, users are able to manually classify assets to each of the available types.

The new list of asset types:

Controllers	Field Devices	OT Devices	OT Servers	Network Devices	Servers	IoT	Workstations	Endpoints
Controller	Field Device	OT Device	OT Server	Network Device	Server	IoT	Workstation	Endpoint
PLC	Actuator	Industrial Printer	Historian	Router	File Server	Camera	OT Workstation	Mobile
DCS	Smart Sensor		HMI	Switch	Web Server	Panel	Engineering Station	
IED	Inverter		Data Logger	Hub	Virtual Server	Projector	Virtual Workstation	
RTU	Relay			Wireless		VOIP Device		

				Access Point				
Communication Module	Remote I/O			Firewall		3D Printer		
I/O Module	Power Meter			Converter		Printer		
CNC				Radio		UPS		
Power Supply				Serial-Ethernet Bridge		IP Phone		
				Gateway		Storage Device		

Integrating Nessus into OT Security

OT Security allows its users to perform a Nessus scan on assets of their choice. This allows them to harness the best of vulnerability assessments for all non-OT specific assets in the OT environment. Subsequently, OT Security can reflect these vulnerabilities to Tenable Security Center and Tenable Vulnerability Management based on the available integrations between them in order to allow for complete vulnerability assessment for all enterprise environments.

Users control over Nessus scans from OT Security is comprehensive as they are launched only on single assets by user-activation only. At the same time, OT Security prevents the execution of Nessus scans on assets which are identified as controllers, field devices and other OT specific devices. In addition it advises the user to take extra care when analyzing OT-related servers, and to consider such scans on maintenance time windows.

New Scan for Ripple20 vulnerabilities identification

OT Security allows its users to perform a scan of their inventory to identify vulnerable devices related to the recently publicly available Ripple20 set of vulnerabilities. This is based on the Nessus plugin which was made available after the disclosure. Users can launch this scan manually and have full control on which assets to scan.

User Managed Intrusion Detection Rule Groups

On top of the existing out-of-the-box intrusion detection policies and available Suricata rules which are organized in predefined rule groups, OT Security now offers extended flexibility in their accommodation to specific environments and circumstance. Users can now review the entire rule repository, which includes both curated and tenable own rules, and create user-defined policies to apply self chosen rules. In addition, the user can add or remove rules from existing threat detection policies in case further adaptation is needed.

PCAP Player

Users can now play network capture files (.pcap, .pcapng, .pcap.gz, .pcapng.gz) to OT Security core platform. This can be used for simulation purpose or in order to analyze traffic that is not taken from the parts of the network that are monitored continuously. Uploading and playing network capture files are available from the PCAP Player page in the settings.

VPR and Threat Intelligence Indicators for CVEs

- **VPR**

  Vulnerability priority rating, the output of Tenable Predictive Prioritization, helps organizations improve their remediation efficiency and effectiveness by rating vulnerabilities based on severity level determined by two components: technical impact and threat. The VPR score is now displayed for each identified CVE, both in the CVEs tab in the single asset page and in the general CVEs table under the Risk tab.

- **VPR Key Drivers**

  For each CVE you can now view the global threat landscape key drivers to explain the CVE's VPR score.

  The following table describes the key drivers:

Key Driver	Description
Vulnerability	The number of days since the National Vulnerability Database (NVD)

Age	published the vulnerability.
CVSSv3 Impact Score	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, OT Security displays a Tenable-predicted score.
Exploit Code Maturity	The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (High, Functional, PoC, or Unproven) parallel the CVSS Exploit Code Maturity categories.
Product Coverage	The relative number of unique products affected by the vulnerability: **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays **No recorded events**.
Threat Intensity	The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Threat Recency	The number of days (0-730) since a threat event occurred for the vulnerability.

- **CVSSv3**

  We are now presenting the Common Vulnerability Scoring System (CVSS) v3 besides the former CVSSv2 and the new VPR score in the CVEs page on the general Risk tab and in the CVEs tab of single assets.

- **Base Scores**

  NVD's base scores are presented per each identified CVE. The base scores are the characteristics of the CVE that are constant with time and across user environments. The Access Vector, Access Complexity, and Authentication metrics capture how the vulnerability is accessed and whether or not extra conditions are required to exploit it. The three impact metrics measure how a vulnerability, if exploited, will directly affect an IT asset, where the impacts are independently defined as the degree of loss of confidentiality, integrity, and availability.

Indicating Purdue Level of Assets

Every asset is now labeled with its level according to the Purdue Model for Computer Integrated Manufacturing. Based on that users can sort, filter and group by their Purdue level. The Purdue level designation of assets are available for users to edit.

Event Based PCAPs from Enterprise Manager

In version 3.5.13 we released the capability of extracting .pcap files filtered from the full network captures to specific events triggered by our policy based engine. We are now enabling this capability from the single site view of the Enterprise Manager as well.

Bug Fixes

Bug Fix
Aruba ClearPass integration - Slowed down the rate of information which is sent to ClearPass.
Report Performance Issues Fixed - Limited number of assets in CVE Drill Down chapter to 20.
Fix wrong units on Top Sources/Destinations Chart on network summary page
Setup Wizard redirected to blank white page (instead of reloading page)
Report with asset drill down information failed to be generated
Packet capture File Management for Sensors behind NAT fix.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

OT Security 3.7.22 Release Notes (2020-09-14)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

To download OT Security upgrade files, see: https://tenable-ot.sharefile.com/d-s9366b39d2974a06b.

For a list of previous versions that are possible to perform a direct upgrade from, see: https://tenable-ot.sharefile.com/d-seef9789fa134f489.

New Features

Basic Active Support

- Andritz Thyne, Lenze IO, MVK Metal IO, Eaton Power Xpert, Ocean Controls KTA, Sick, Comet, Silex Technology and other IOT devices.

Bug Fixes

Bug Fix
Missing Sync Now on Tenable Vulnerability Management and Tenable Security Center Integrations
Adding Nessus Scan Results to Tenable Vulnerability Management and Tenable Security Center Integration
Fix Issue with Split Ports
Fix Issue of limited option to Copy & Paste from Grids
Fix CVE Matching for Yokogawa https://us-cert.cisa.gov/ics/advisories/icsa-20-224-01
Enable special characters for SMTP password
Fix setting date and time manually, the time sent should be in UTC (time configured - timezone)
Fix user unable to delete DNS server after it was entered
Fix run now should be disabled when no CIDRs are entered
Fix user allow to send empty SNMP V3 form
Fix Network Summary default time value was browser GMT without calculating time zone

API Changelog

For more information about the API changes for this release, see the OT Security API Changelog.

Filenames and MD5 Checksums

File	MD5
cobex_3.7.22.tar.xz.gpg	a2fa4e66b0916748aa5e0ef4b2a4a010

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

OT Security 3.8.13 Release Notes (2020-10-08)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

To download OT Security upgrade files, see: https://tenable-ot.sharefile.com/d-s1fd50e753e84da29.

For a list of previous versions that are possible to perform a direct upgrade from, see: https://tenable-ot.sharefile.com/d-s6aa49a309774c14a.

New Features

Attack Vectors

OT Security will now allow users to perform predictive attack analysis by calculating potential attack vectors for each asset. An attack vector is a communication path that an attacker might use to reach a given asset in the network, by leveraging network connectivity and vulnerabilities of assets along the way.

It's presented in the single asset details page, in a dedicated new sub-tab, that can be accessed via the navigation bar.

The user can either choose a specific asset as a potential starting point for the attack or leave it up to the system to identify the most critical vector.

Matching Tenable User Interface Look and Feel

The OT Security user interface now matches the rest of the Tenable product suite, particularly Tenable Vulnerability Management.

Integrations with Tenable Security Center and Tenable Vulnerability Management can now be configured via the user interface

The respective configurations can be found in the ICP local settings tab. The user can set the frequency of data posting.

Cache for Syslog Messages

Syslog messages that are sent over TCP are now being cached in case of communication failures, to address syslog servers (e.g. SIEM systems) that are temporarily down. Cache size is up to 10,000 messages.

Detection of Vulnerabilities in Wibu's CodeMeter

A predefined policy was added, aimed at flagging devices that are susceptible to vulnerabilities in Wibu's CodeMeter license manager, which is used by several industrial automation vendors. The policy is based on a Suricata rule released by the research team, in response to the CISA advisory on this matter.

Vendor Support

ABB AC500 - Basic Passive and Standard Active support were added.

Leveraging FTP Responses for Asset Fingerprinting

Asset details are extracted and used for fingerprinting and classification.

Bug Fixes

Bug Fix
Integration of Tenable Vulnerability Management require server key on any update

Suricata configuration for Dell PoweEdge HW
User failed to delete group after used in complex group
Ignore RDP events when are executed from the box (as part of Nessus)

API Changelog

For more information about the API changes for this release, see the OT Security API Changelog.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

OT Security 3.8.15 Release Notes (2020-10-16)

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

To download OT Security upgrade files, see: https://tenable-ot.sharefile.com/d-s68d7ab484d04a549.

For a list of previous versions that are possible to perform a direct upgrade from, see: https://tenable-ot.sharefile.com/d-s488331a631b4e90b.

Bug Fixes

Bug Fix
Fixed migration issue to 3.8 GA.

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Nessus	8.10.1 and later

OT Security 3.8.17 Release Notes (2020-11-09)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

To download OT Security upgrade files, see: https://tenable-ot.sharefile.com/d-sa3d6ad208a314ad.

For a list of previous versions that are possible to perform a direct upgrade from, see: https://tenable-ot.sharefile.com/d-s6fa9363d35ba4f8.

Bug Fixes

Bug Fix
Post Factory reset system failed to initialize
Spike in conversation event, conversation deviation numbers divided by 100
After editing SNMP server, empty password is sent and the server is not working
Events that are already resolved displayed in the events tab on single asset page
Generate vector on external assets should not be presented
Attack Vector - Auto Generated Failed with error "no available source for destination" as all src assets in graph have Risk score 0
Reconnaissance tools needs libpcap (debian) and is not runnable
Email links in report presented with ICP IP address instead of config url

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)

Tenable Security Center	5.11 and later
Tenable Nessus	8.10.1 and later

OT Security 3.9.14 Release Notes (2020-12-15)

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

To download OT Security upgrade files, see: https://tenable-ot.sharefile.com/d-s5fe55420c492418cbced071043cfd9c6.

For a list of previous versions that are possible to perform a direct upgrade from, see: https://tenable-ot.sharefile.com/d-s832ad21b0b8647f7948e2d57d59e5b81.

New Features

Network Map Redesign

OT Security's network map was rebuilt. Alongside an improved user experience, the user can now easily group and filter assets by their type, vendor, or risk level. This helps to make the map more useful, especially for large numbers of assets.

Increased IoT Visibility

OT Security now identifies various IoT devices. If these devices are detected, they are shown in a new designated sub-tab.

New Asset Types

OT Security now identifies the following device types:

Category	New Type
IoT	Access Control System
IoT	HVAC Module
IoT	Lighting Control
IoT	Smart Hub
IoT	Smart TV

IoT	Tablet
IoT	Medical Device
Field Device	Barcode Scanner
Field Device	Industrial Sensor
Field Device	Drive
Server	Domain Controller
Network Device	Repeater
OT Device	Industrial Router
OT Device	Industrial Switch
OT Device	Industrial Gateway
OT Device	Industrial Network Device

Saia PCD - Standard Active Support

OT Security now detects the device model, firmware version, hardware version, CPU state, and the project name of SAIA PCD devices. This support level in particular facilitates the detection of their vulnerabilities.

Basic Active Support for Various Assets

Basic active support was added for the following devices:

- Schneider PowerLogic EGX100 Gateway
- Digi One SP Serial-Ethernet Bridge
- Westermo EDW-1x0 Serial-Ethernet Bridge
- Tait Communications TB9x00 DMR Base Station
- Eaton 5PX UPS

Sync Now Tenable Security Center and Tenable Vulnerability Management

Pushing data from OT Security to Tenable Security Center and Tenable Vulnerability Management can now be done on-demand via the user interface.

Conversations Log

The conversations log has been extended to include 10,000 records.

Bug Fixes

Bug Fix
Factory Reset change "nessusfile" folder permission, preventing IO/SC integration to work
Asset removal scripts failed on version 3.8.x
ControlLogix and CompactLogix missing IOs on AB rack
Factory reset with split port doesn't reset nics configuration

Integrated Tenable Product Compatibility

The following table lists the Tenable product versions tested with this version of OT Security.

Product	Tested Version(s)
Tenable Security Center	5.11 and later
Tenable Nessus	8.10.1 and later

Tenable Security Center Release Notes

To view EOL Tenable Security Center release notes, see Tenable EOL Release Notes.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

View the following Tenable Security Center (formerly Tenable.sc) release notes:

- EOLTenable Security Center 2024 Release Notes
- EOLTenable Security Center 2023 Release Notes
- Tenable Security Center 2022
- Tenable Security Center 2021
- Tenable Security Center 2020
- 2019 Tenable Security Center
- 2018 Tenable Security Center
- 2017 Tenable Security Center
- 2016 Tenable Security Center
- 2015 Tenable Security Center
- 2014 Tenable Security Center
- 2013 Tenable Security Center
- 2012 and Earlier Tenable Security Center

EOLTenable Security Center 2024 Release Notes

Tip: You can subscribe to receive alerts for Tenable documentation updates.

These release notes are listed in reverse chronological order. To jump to a place in the release notes, use the list to the right.

Tenable Security Center Patch 202403.1-6.1.1 (2024-03-25)

Apply this patch to Tenable Security Center installations running versions 6.1.1. This patch updates SQLite to 3.44.0 to address CVE-2023-7104 and CVE-2024-1367.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

   > **Note:** If Tenable Security Center does not automatically restart, then you may need to restart Tenable Security Center manually.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- fileIntegrityHashGenerator.php
- install.sh
- /opt/sc/bin/agent_prepareassets
- /opt/sc/bin/ipv4_prepareassets
- /opt/sc/bin/ipv6_prepareassets
- /opt/sc/bin/universal_prepareassets
- /opt/sc/bin/showvulns
- /opt/sc/bin/showvulns-archive
- /opt/sc/bin/showvulns-individual
- /opt/sc/bin/showvulns-mobile
- /opt/sc/support/bin/sqlite3
- /opt/sc/support/lib/libsqlite3.la
- /opt/sc/support/lib/libsqlite3.a
- /opt/sc/support/lib/libsqlite3.so.0.8.6
- /opt/sc/src/lib/AssetLib.php
- /opt/sc/src/DebugLogs.php
- /opt/sc/src/lib/ResponseHandlerLib.php

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202403.1-5.23.1 (2024-03-25)

Apply this patch to Tenable Security Center installations running versions 5.23.1. This patch updates SQLite to 3.44.0 to address CVE-2023-7104 and CVE-2024-1367.

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

   Note: If Tenable Security Center does not automatically restart, then you may need to restart Tenable Security Center manually.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- fileIntegrityHashGenerator.php
- install.sh

- /opt/sc/bin/agent_prepareassets
- /opt/sc/bin/ipv4_prepareassets
- /opt/sc/bin/ipv6_prepareassets
- /opt/sc/bin/universal_prepareassets
- /opt/sc/bin/showvulns
- /opt/sc/bin/showvulns-archive
- /opt/sc/bin/showvulns-individual
- /opt/sc/bin/showvulns-mobile
- /opt/sc/support/bin/sqlite3
- /opt/sc/support/lib/libsqlite3.la
- /opt/sc/support/lib/libsqlite3.a
- /opt/sc/support/lib/libsqlite3.so.0.8.6
- /opt/sc/src/lib/AssetLib.php
- /opt/sc/src/DebugLogs.php
- /opt/sc/src/lib/ResponseHandlerLib.php

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

EOLTenable Security Center 2023 Release Notes

These release notes are listed in reverse chronological order. To jump to a place in the release notes, use the list to the right.

Tenable Security Center Patch 202312.1-5.23.1 (2023-12-14)

Apply this patch to Tenable Security Center installations running version 5.23.1. This patch updates Apache HTTP Server to version 2.4.58 to address CVE-2023-43622 and CVE-2023-45802.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

   > **Note:** If Tenable Security Center does not automatically restart, then you may need to restart Tenable Security Center manually.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- apr.exp
- aprutil.exp
- httpd
- install.sh
- libapr-1.a
- libapr-1.la
- libapr-1.so.0.7.3
- libaprutil-1.a
- libaprutil-1.la
- libaprutil-1.so.0.6.3

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202310.1-6.x (2023-10-31)

Apply this patch to Tenable Security Center installations running versions 6.0.0, 6.1.0, and 6.1.1. This patch updates curl to version 8.4.0 to address CVE-2023-38545.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

   > **Note:** If Tenable Security Center does not automatically restart, then you may need to restart Tenable Security Center manually.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- install.sh
- libcurl.a
- libcurl.la
- libcurl.so
- libcurl.so.4
- libcurl.so.4.8.0

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202310.1-5.23.1 (2023-10-31)

Apply this patch to Tenable Security Center installations running version 5.23.1. This patch updates curl to version 8.4.0 to address CVE-2023-38545.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

   > **Note:** If Tenable Security Center does not automatically restart, then you may need to restart Tenable Security Center manually.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- install.sh
- libcurl.a
- libcurl.la
- libcurl.so
- libcurl.so.4
- libcurl.so.4.8.0

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202307.1-6.x (2023-07-25)

Apply this patch to Tenable Security Center installations running versions 6.0.0, 6.1.0, and 6.1.1. This patch updates OpenSSL to version 3.0.9 to address CVE-2023-2650.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- install.sh
- libcrypto.a
- libcrypto.so
- libcrypto.so.1.1
- libssl.so
- libssl.so.1.1
- openssl

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202307.1-5.23.1 (2023-07-25)

Apply this patch to Tenable Security Center installations running version 5.23.1. This patch updates OpenSSL to version 1.1.1u to address CVE-2023-2650.

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- install.sh
- libcrypto.a
- libcrypto.so
- libcrypto.so.3

- libssl.so
- libssl.so.3
- openssl

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 6.1.1 (2023-06-07)

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.12.0 or later, you can upgrade directly to Tenable Security Center 6.1.1. If you are running a version earlier than Tenable Security Center 5.12.0, upgrade to Tenable Security Center 5.12.0 before upgrading to Tenable Security Center 6.1.1.

If you are running Tenable Security Center 6.1.1 and you are using pyTenable with the Tenable Security Center API, you must upgrade pyTenable to version 1.4.2 or later.

If you upgrade Tenable Security Center Director, upgrade Tenable Security Center for all managed Tenable Security Center instances connected to Tenable Security Center Director. After upgrading, allow up to 15 minutes for your managed Tenable Security Center instances to sync with Tenable Security Center Director.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** If your upgrade path skips versions of Tenable Security Center (for example, upgrading from 5.20.0 to 5.23.1 to 6.1.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

> **Note:** Tenable Security Center 5.21.0 is the last version of Tenable Security Center that supports Internet Explorer. For more information about other supported browsers, see Web Browser Requirements in the *Tenable Security Center User Guide*.

New Features

MaaS360 MDM Integration

Tenable Security Center customers can now create MaaS360 MDM mobile repositories.

For more information, see Mobile Repositories in the *Tenable Security Center User Guide*.

Security Updates

Updated Tenable Security Center to remove support for weaker, legacy cipher suites.

Bug Fixes

Bug Fix	Defect ID
When syncing assets lists from Tenable Security Center to Tenable Vulnerability Management, updated the request payload so that filter values are chunked to contain no more than 1024 values per filter. Customers can now sync asset lists from Tenable Security Center to Tenable Vulnerability Management tags successfully when they contain more than 1024 filter values (IPs, FQDNs, and Tenable UUIDs).	01597028
Tenable Security Center was updated to maintain asset information in the case when all cumulative vulns have expired but there are some mitigated vulns remaining.	01570011, 01585371, 01604201
Updated diagnostics so that all system calls run successfully with the output results shown in *sc-systeminfo.txt* within the diagnostic file. A diagnostic can now be successfully run in EL7, 8, and 9 environments.	01584035
Fixed issue with asset calculation in Universal repository when a referenced asset no longer existed.	01548973, 01593435, 01612646
Fixed bug in asset list count for Universal repository that occurred when there was more than one asset with the same FQDN in the repository.	01557339, 01589415
Fixed an issue that caused an "API Keys not accepted" error for agent scans on agent manager.	01534931, 01540595,

	01561334
When editing an asset on a large repository with many groups and a large user base, the internal error 500 occurs. Now this has been resolved.	01531118, 01555418

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 6.1.1.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.9.0 and later
OT Security	3.9.25 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.11.0 and later

Tenable Security Center Patch 202304.1 (2023-04-25)

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.22.0, 5.23.1, and 6.0.0. This patch updates PHP to version 8.1.16 to address CVE-2023-0568 and CVE-2023-0662.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- php

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202304.0 (2023-04-12)

Apply this patch to Tenable Security Center installations running Tenable Security Center 6.1.0.

This patch resolves an issue with synchronization using Tenable One/Tenable Lumin, where Agent UUIDs with dashes in Asset Lists created issues with Tag definitions.

Steps to Apply Patch through the Tenable Security Center Feed

If you are running Tenable Security Center 6.1.0 and have enabled updates through the feed, this patch will be applied automatically.

To enable updates through the Tenable Security Center feed:

1. Log in to Tenable Security Center as an Administrator.
2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.
3. Click the **Plugins/Feed** tile.

   The **Plugins/Feed Configuration** page appears.
4. On the **Plugins/Feed Configuration** page, in the **Tenable Security Center Software Updates** section, enable the **Enable Updates Through the Tenable Security Center Feed** option.

   During the next scheduled feed update, Tenable Security Center applies the patch. In the **Tenable Security Center Software Updates** table, a timestamp appears in the row for the patch in the **Last Updated** column.

Steps to Apply Patch Manually

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- httpd
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202303.2 (2023-03-28)

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.22.0, 5.23.1, and 6.0.0. This patch updates Apache HTTP Server to version 2.4.56 to address CVE-2023-25690.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- httpd
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 6.1.0 (2023-03-22)

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.12.0 or later, you can upgrade directly to Tenable Security Center 6.1.0. If you are running a version earlier than Tenable Security Center 5.12.0, upgrade to Tenable Security Center 5.12.0 before upgrading to Tenable Security Center 6.1.0.

If you are running Tenable Security Center 6.1.0 and you are using pyTenable with the Tenable Security Center API, you must upgrade pyTenable to version 1.4.2 or later.

If you upgrade Tenable Security Center Director, upgrade Tenable Security Center for all managed Tenable Security Center instances connected to Tenable Security Center Director. After upgrading, allow up to 15 minutes for your managed Tenable Security Center instances to sync with Tenable Security Center Director.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** If your upgrade path skips versions of Tenable Security Center (for example, upgrading from 5.20.0 to 5.23.1 to 6.1.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

> **Note:** Tenable Security Center 5.21.0 is the last version of Tenable Security Center that supports Internet Explorer. For more information about other supported browsers, see Web Browser Requirements in the *Tenable Security Center User Guide*.

New Features

Global Search for Assets

Tenable Security Center customers can now use the Global Search feature to search for host assets by IPv4.

For more information, see Search in the *Tenable Security Center User Guide*.

Domain Inventory Filtering

Tenable Security Center customers can now filter their domain inventory assets.

For more information, see Domain Inventory Filter Components in the *Tenable Security Center User Guide*.

Linked Users for Non-Admin Accounts

Tenable Security Center customers can now create linked users for Security Manager user accounts.

For more information, see Linked User Accounts in the *Tenable Security Center User Guide*.

Bulk ACR Edit

Tenable Security Center customers can now edit multiple ACR values at a time.

For more information, see Edit an ACR Manually in the *Tenable Security Center User Guide*.

Recast Expiration Date

Tenable Security Center customers can now set expiration dates for recast rules.

For more information, see Add a Recast Risk Rule in the *Tenable Security Center User Guide*.

Tenable One Data Reliability

For customers using the Lumin Connector, Tenable Security Center data in Lumin is now far more reliable as Tenable One now recognizes the host UUID generated by Tenable Security Center.

For more information, see Tenable One Synchronization in the *Tenable Security Center User Guide*.

Notification Bell Icon

The Tenable Security Center header now includes a notification bell, which alerts users of important notifications.

For more information, see Notifications in the *Tenable Security Center User Guide*.

Wildcards in NetBIOS Name Filter

Tenable Security Center customers can now user wildcards and regular expressions in the Vulnerability Analysis NetBIOS Name filter.

For more information, see Vulnerability Analysis Filter Components in the *Tenable Security Center User Guide*.

Delinea Secret Server PAM

Tenable Security Center now supports the Delinea Secret Server PAM authentication method.

For more information, see Windows Credentials, SSH Credentials, and Privilege Escalation in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

Added commas to numbers with four or more digits to make them easier to read.

Bug Fixes

Bug Fix	Defect ID
A POST request to create a policy requires that the state (mixed or enabled), and the type (locked or unlocked for a state of mixed, and always unlocked for a state of enabled) be included for each family in the request.	01558364
Added a fix where "Create Plugin scans" is not visible if "Create Scan" is disabled on initial loading of a custom role edit.	01553947
Corrected how Tenable Security Center determines if the data is ready to refresh.	01509109
PDFs are no longer encrypted by default. The 'Encrypt PDF' option must be enabled before a PDF is encrypted.	01549696
Fixed issues handling and accounting for early, requested pauses, resumes and stops within the active scan process.	01546822
Fixed loading of AES/ACR from database.	01546444
This fixes a bug where the code was crashing if the user used an external SC API and did not provide a User Agent header.	01538318
Fixed issue where users were unable to copy Dashboard components to Dashboard tabs that they manage but not own.	01401206
Added a sort compare function for the risk reduction column and will sort properly in the dashboard component "Worst of the worst - Top 10 prioritized actions"	01513870
Fixed issue where column "IP/Device Count" did not sort properly in	01524451

Repositories list view.	
Improvements made to mobile scans to prevent timeouts.	01435903
Fixed user privileges for scan results view to have pause and stop button enabled for the scans created by that user, even without MO enabled.	01512444
typeFields was not handled properly for few credential types. Now all supported credential types support typeFields.	01489431
Optimization of backend queries during the SC feed process. This saves PHP memory and prevents PHP 'out of memory' issues.	01510611, 01508444, 01532158, 01537509
When creating a scan policy, setting "Search for DTLS" to anything other than 'None' saves correctly now.	01503411
Fixed an issue where importing a scan causes a "license check failed" error.	01501139, 01515264
Fixed an issue where column "Owner" did not sort properly in Active Scans list view.	01498956
Fixed an issue where old scan results were not being cleaned up when an expiration lifetime was configured.	01488760
Large Tenable Security Center Debug logs will no longer throw memory related issues.	01493694, 01497471, 01550915
Fixed an issue where the post-scan report was not generated if the active scan was created via API.	01439481

Known Issues

- The **Address** filter on the **Domain Inventory** page allows users to enter invalid values.
- Some instances of Tenable Lumin still appear in the UI, instead of Tenable One.

- If a user views the **View Scan Result** page while a scan is running, an error may appear in the admin log. This will not affect the scan.
- There is a cosmetic UI issue with overflowing borders on the **Add Dynamic Asset** page.
- There can be discrepancies between vulnerability data in Tenable Security Center and Tenable Vulnerability Management when vulnerabilities for dead hosts are removed from the cumulative database.

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 6.1.0.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.9.0 and later
OT Security	3.9.25 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.11.0 and later

Tenable Security Center Patch 202303.1-6.x (2023-03-01)

Apply this patch to Tenable Security Center installations running version 6.0.0. This patch updates OpenSSL to version 3.0.8 to address the following vulnerabilities:

- CVE-2022-4304
- CVE-2023-0215
- CVE-2022-4450
- CVE-2023-0216
- CVE-2023-0217
- CVE-2023-0401
- CVE-2022-0403

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- libcrypto.a
- libcrypto.so
- libcrypto.so.3
- libssl.so
- libssl.so.3
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202303.1-5.x (2023-03-01)

Apply this patch to Tenable Security Center installations running version 5.23.1. This patch updates OpenSSL to version 1.1.1t to address the following vulnerabilities:

- CVE-2022-4304
- CVE-2023-0215
- CVE-2022-4450

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- libcrypto.so.1.1
- libssl.so.1.1
- openssl
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202302.3 (2023-02-21)

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.22.0 and 5.23.1. This patch updates libCurl to version 7.86.0 to address CVE-2022-42916.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- libcurl.a
- libcurl.la
- libcurl.so.4.8.0
- liblber.so.2.0.200
- libldap.so.2.0.200
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202302.2 (2023-02-21)

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.22.0, 5.23.1, and 6.0.0. This patch updates Apache HTTP Server to version 2.4.55 to address CVE-2022-37436.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- httpd
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202302.1 (2023-02-07)

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.23.1. This patch fixes an issue where some users see a "scan progress not showing in Scan Results page" error while scanning.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from the Tenable Security Center Downloads page to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- html/index.html
- html/main.52a1ec78d7f29ac9bc2d.js
- SCILib.php
- style.css
- darkmode.css
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 6.0.0 (2023-01-25)

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.12.0 or later, you can upgrade directly to Tenable Security Center 6.0.0. If you are running a version earlier than Tenable Security Center 5.12.0, upgrade to Tenable Security Center 5.12.0 before upgrading to Tenable Security Center 6.0.0.

If you are running Tenable Security Center 6.0.0 and you are using pyTenable with the Tenable Security Center API, you must upgrade pyTenable to version 1.4.2 or later.

If you upgrade Tenable Security Center Director, upgrade Tenable Security Center for all managed Tenable Security Center instances connected to Tenable Security Center Director. After upgrading, allow up to 15 minutes for your managed Tenable Security Center instances to sync with Tenable Security Center Director.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

This release includes an upgrade to OpenSSL 3.0.x. This resolves two issues found in the open source libraries, CVE-2021-3450 and CVE-2021-3449. Both issues were rated High. As a result, X.509 certificates signed using SHA1 are no longer allowed at security level 1 or higher. The default security level for TLS is 1, so certificates signed using SHA1 are by default no longer trusted to authenticate servers or clients. Customers who encounter this issue should upgrade their certificates. For more information, see the OpenSSL 3.0 release notes.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** If your upgrade path skips versions of Tenable Security Center (for example, upgrading from 5.9.0 to 5.12.0 to 6.0.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

> **Note:** Tenable Security Center 5.21.0 is the last version of Tenable Security Center that supports Internet Explorer. For more information about other supported browsers, see Web Browser Requirements in the *Tenable Security Center User Guide*.

New Features

New Look and Feel

The Tenable Security Center look and feel has been modernized by updating the typography, navigation, login screen, and more.

OpenSSL 3.0 Support

Tenable Security Center now supports OpenSSL 3.0.

Oracle Linux 9 and Red Hat Enterprise Linux (RHEL) 9 Support

Added support for Oracle Linux 9 and RHEL 9. Tenable Security Center will continue to support CentOS 7, RHEL 7, and RHEL 8.

For more information, see System Requirements in the *Tenable Security Center User Guide*.

Dashboard Matrix Default Color Swatches

Tenable Security Center customers can now select from a group of default colors when editing dashboard matrix component rules.

For more information, see Custom Dashboard Component Options in the *Tenable Security Center User Guide*.

Scan Policy Plugin Management

Tenable Security Center customers can now add and enable plugins in mixed plugin families.

For more information, see Configure Plugin Options in the *Tenable Security Center User Guide*.

Updating Tenable Security Center Patches Through the Feed

Tenable Security Center customers can now download and install patches directly inside the Tenable Security Center console. There is a new option to automatically install patches with feed updates.

For more information, see Configuration Settings in the *Tenable Security Center User Guide*.

Health Overview Dashboard

Tenable Security Center has a new Health Overview dashboard that provides quick access to deployment issues. Tenable Security Center customers can use this dashboard to gain better insight and understanding of their Tenable Security Center infrastructure.

For more information, see Health Overview Dashboard in the *Tenable Security Center User Guide*.

Password Expiration

Tenable Security Center administrative users can now set password expiration settings for users.

For more information, see User Account Options in the *Tenable Security Center User Guide*.

Current/Previous Year Filter

The **Time** filter in Tenable Security Center now includes the **Current Year** and **Last Year** options.

For more information, see Vulnerability Analysis Filters in the *Tenable Security Center User Guide*.

Wallix Bastion PAM

Tenable Security Center now supports the Wallix Bastion PAM authentication method.

For more information, see Database Credentials Authentication Method Settings in the *Tenable Security Center User Guide*.

Global Search

Tenable Security Center customers can now search for vulnerabilities by CVE.

For more information, see Search in the *Tenable Security Center User Guide*.

Increased PDF Encryption Strength

Tenable Security Center customers can now encrypt PDF reports using a 256 bit AES algorithm.

For more information, see Report Options in the *Tenable Security Center User Guide*.

Update Asset List before Running Dependent Scans

In Tenable Security Center if a dependent scan is using a dynamic asset list, that asset list will now be updated before the scan runs.

For more information, see Assets in the *Tenable Security Center User Guide*.

NetBIOS Filter

Tenable Security Center customers can now filter vulnerabilities by NetBIOS name.

For more information, see Vulnerability Analysis Filter Components in the *Tenable Security Center User Guide*.

Universal Repository

Tenable Security Center customers have access to the new Universal repository type, which can store data from IPv4, IPv6, and Agent repositories.

For more information, see Universal Repositories in the *Tenable Security Center User Guide*.

CyberARK Credential Updates

Tenable Security Center customers that use CyberArk credentials can now use **Address** for the **Get Credentials By** setting.

For more information, see SSH Credentials in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

Performance improvements for Tenable Security Center Director and syncing repositories.

Bug Fixes

Bug Fix	Defect ID
Fixes a race condition on login that may have caused incorrect permissions for the logged-in user under poor network conditions.	01504937
Fixed an issue with sorting accept rules by Creator.	01494988
Fixed issues related to chunk deletion and chunk re-injection when scanners go offline during a scan.	01490102, 01496734, 01529623, 01536174
Stopped using recursion to process combination asset lists to prevent using up stack memory.	01485883, 01479281, 01509793, 01475287
The SC feed was updated to exclude the AD Identity Scan policy template.	01483391
Removed *.cloudfront.net from the CSP request header. The domain was previously added to download content for Pendo, but now all external resources are served from a Tenable domain.	01483322
Fixed an issue where large scan result imports were failing by removing database locks.	01482303
Fixed a dashboard query error with the Output Assets filter.	01480528
Fixed an issue so the agentScan API returns agentGroups field information upon request. `agentScan?fields=agentGroups::GET`	01478230
Fixed an issue where selecting the Initiator column would not properly sort the job queue.	01474973
Fixed an issue where the Licensing Status dashboard widget appeared blank.	01471612, 01479097, 01468610, 01517641
Fixed an issue where if the diagnostic scan failed, the diagnostic scan	01470275

password was not sanitized in the system log.	
Fixed the backup and restore config tools to correctly backup and restore compliance plugin data. This was resolved by accounting for an offset in row IDs between the backup and restore box, particularly plugin external reference data.	01469141
Introduced the new Time filter with Created and Finished options to replace the Completion Time filter.	01467850, 01477190, 01481914, 01506659, 01466750, 01524139, 01536947
Fixed an issue where Asset bulk delete throws an error. A condition has been added to `/asset/id::DELETE` to verify `JobLib::getIgnoreAddingNewJobsStatus()`. If the **Ignore adding new job** option is enabled, we return the response without looking for the affected group.	01459697, 01479181, 01497531, 01523580
Fixed an issue when using the import option in IBM DB2 credentials where the client certificates entered in the Legacy CyberArk credentials screen were not retained after saving the details.	01455757
Fixed an issue where the last item in the data grid(tabulator) could not be accommodated when classification is mentioned. The issue is fixed by modifying the logic to calculate the height for the new screens appropriately to contain the classification and removing the "!important" in the css.	01451953
Fixed an issue where system logs would not scroll beyond the selected month. This was resolved by changing the design of the table. System logs are now in a paginated list, instead of an infinite scroll paradigm.	01449648, 01475247
Fixed an issue where clicking the dashboard component with Query Value: Hosts would take the user to the wrong tool in Vulnerability Analysis. The user now lands correctly on the Vulnerability List.	01449110

Fixed an issue where a query error would appear in Vulnerability Analysis after deleting a scan result. The issue was fixed by adding a check to find if the scan result exists in the system, then loading the view based on that.	01443526
Fixed an issue where the automatic refresh on the **Scan Results** page did not save the user's scroll position in the table,	01442405, 01507580, 01518858
Fixed an issue where a Tenable Nessus Compliance Scan import failed, despite a success message from Tenable Security Center.	01436887
Fixed an issue where dashboard components were referencing invalid queries, making users unable to edit the dashboard components.	01406788
Fixed an issue where the **Owner** filter on the **Report Results** page would show multiple instances of the same owner name.	01400225
Fixed an issue where the file `/opt/sc/support/etc/SimpleSAML/config/config.php` could be overwritten during a Tenable Security Center upgrade.	01385220
Reduced the time and accuracy of the List Software tool to calculate results from updates made to Plugin #22869 and Plugin #20811.	01382651

Known Issues

- When an admin creates a new user, the Switch User option doesn't show up immediately after creating the linked user.
- When the browser window is resized, Line Chart components will not resize appropriately to fit their respective containers.
- When zooming in on the browser, some elements in the header may no longer be visible.
- Pendo is reporting an incorrect date format in the SC productExpirationDate metadata.
- Safari SC users will see shadows of the left navigation after clicking.
- When in any Analysis view, the Analysis icon in SideNav should have a blue background with a dark blue line to the left.

- Creating a risk rule doesn't work for certain combinations for fields and repositories. For example, creating a risk rule with an IP as the identifier doesn't work for an Agent repo.
- Pagination icons should appear grayed out when they are unusable, for example, when there is only 1 page of results.
- Universal repository is not available in the Quick Setup Guide.

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 6.0.0.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.9.0 and later
OT Security	3.9.25 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.11.0 and later

Tenable Security Center 2022

Tenable Security Center 5.20.0 Release Notes (2022-01-05)

Tenable Security Center Patch 202201.1 Release Notes (2022-01-12)

Tenable Security Center 5.20.1 Release Notes (2022-01-24)

- Tenable Security Center Patch 202202.1 Release Notes (2022-02-01)
- Tenable Security Center Patch 202203.1 Release Notes (2022-03-03)
- Tenable Security Center Patch 202203.2 Release Notes (2022-03-09)
- Tenable Security Center Patch 202204.1 Release Notes (2022-04-06)
- Tenable Security Center 5.23.1 Release Notes (2022-09-15)
- Tenable Security Center Patch 202209.2 Release Notes (2022-09-22)

Tenable Security Center 5.20.0 Release Notes (2022-01-05)

> **Note:** Tenable recommends upgrading to the patch for this release, Tenable Security Center Patch 202204.1, which includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.12.0 or later, you can upgrade directly to Tenable Security Center 5.20.0. If you are running a version earlier than Tenable Security Center 5.12.0, upgrade to Tenable Security Center 5.12.0 before upgrading to Tenable Security Center 5.20.0.

If you are using Internet Explorer 11 on Windows 10 LTSB (build 14393.4104), you may need to add your Tenable Security Center installation to the “Trusted Sites” zone in order for the application to load.

If you are running Tenable Security Center 5.20.0 and you are using pyTenable with the Tenable Security Center API, you must upgrade pyTenable to version 1.4.2 or later.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.9.0 to 5.12.0 to 5.20.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Tenable Security Center Director

New Features

Asset Host View

Added a Host View table where you can see details about the asset, associated findings (vulnerabilities), and the associated software inventory.

For more information, see View Hosts in the *Tenable Security Center User Guide*.

Asset Criticality Rating (ACR)

Added in automatic calculation of Asset Criticality Rating (ACR) to be used as part of a Risk Based Approach to Vulnerability Management. Automatic ACR calculation can also be overridden to reflect the most accurate picture of each of your Assets criticality to your environment. ACR can be used throughout Tenable Security Center. Note this feature requires a Tenable Security Center+ license.

> **Note:** As part of the initial ACR score calculation which occurs after the initial Tenable Security Center 5.20.0 installation or upgrade, you must re-scan each host to ensure that Tenable Security Center has the data required to calculate an ACR score. Until that re-scan has been completed, some hosts may not have an ACR score assigned.

UI Improvements

To give our users a more updated and consistent experience across Tenable products, we have made the following enhancements:

- Single button to refresh all dashboard components
- Dashboard enhancements and modernization
- Tab modernization throughout Tenable Security Center
- Enhanced template creation experience
- Enhanced filter experience
- Dark mode severity colors update to align with light mode color scheme

Manage Tenable Nessus Scanners in Tenable Security Center

Added the ability to manage the Tenable Nessus scanners directly in the Tenable Security Center UI.

For more information, see Picture in Picture in the *Tenable Security Center User Guide*.

Backup and Restore Tenable Security Center Configuration Data

Added the ability to backup and restore Tenable Security Center configuration data.

For more information, see Configuration Backups in the *Tenable Security Center User Guide*.

Advanced Agent Scan Policy

Added support for adding an Advanced Agent Scan Policy directly in Tenable Security Center.

For more information, see Agent Scans in the *Tenable Security Center User Guide*.

Tenable Security Center File Integrity Check

Added the ability to check the integrity of critical Tenable Security Center files.

For more information, see Diagnostics Settings in the *Tenable Security Center User Guide*.

Enhanced Diagnostics

Added additional output items to the diagnostics capability of Tenable Security Center.

For more information, see Diagnostics File Options in the *Tenable Security Center User Guide*.

Updated Third Party Integrations

The following integrations have been enhanced:

- Tenable Security Center now works with the CyberArk 2.0 APIs
- Tenable Security Center now allows for credential support when assessing MongoDB

For more information, see SSH Credentials, Windows Credentials, and Database Credentials in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

Display Name in Plugin 19506

Tenable Security Center now shows the scan name in Plugin 19506.

Deprecated Shibboleth 1.3

Tenable Security Center no longer supports Shibboleth 1.3. Shibboleth 2.0 continues to be supported.

Deprecated Scan Policy Templates

Tenable Security Center 5.20.0 no longer supports the following scan policy templates:

- Badlock detection
- Bash Shellshock detection
- DROWN detection
- Shadow Brokers Scan

You cannot create a new scan policy using a deprecated template using the Tenable Security Center UI or API. If you have an existing scan policy using one of these deprecated templates, you can continue to view, edit, and use the templates in scans.

Security Updates

- Removed the SecurityCenter Version header from all Tenable Security Center API calls to prevent unauthorized users from determining the currently running Tenable Security Center version.

Bug Fixes

Bug Fix	Defect ID
Fixed an issue where upgrading to Tenable Security Center 5.19 resulted in a database backup error.	01243705
Corrected an issue where the Plugin Timestamp was displaying incorrectly.	01289970
Corrected an issue when selecting an invalid interval on the scheduling API caused a job daemon to crash.	01276243
Fixed a discrepancy when using filtering in asset lists.	01263324
Fixed an issue where Invalid Scan Zones was reported after re-adding a scanner.	01260386
Corrected an issue where the % usage of repository size was showing incorrectly.	01274320
Corrected an issue syncing Dynamic Assets to Tenable Vulnerability	01251591

Management Tags when the Tenable Vulnerability Management Networks feature is disabled.	
Corrected an issue where the status of Tenable Network Monitor scanners initially displays incorrectly in the Options -> Update Status screen.	01267931
Corrected an issue in Tenable Security Center Director which resulted in a Fingerprint Mismatch or Protocol Error.	01266404
Corrected a Remote Repository sync issue that occurred in rare instances under certain conditions.	01246158
Fixed an issue leading to query errors in the Vulnerability Analysis drill downs when a selected filter returned no matches.	01194875
Corrected an issue that was causing an internal port range error on the Internal PCI Audit Template.	01248527
Fixed an issue where other installations could no longer set up remote agent repositories against the current one.	01252376
Corrected an issue where under certain circumstances a regular user could view the User page.	01252321
Resolved an issue when building an SCAP results file against a large number of hosts.	01246830
Corrected a display issue when rendering a large amount of reports in the Report Results page.	01248675
Corrected an issue where a report would not generate correctly under certain circumstances.	01245189
Resolved an issue where the Output Asset Filter was removed when browsing Dashboard Component Data.	01220853
Corrected an issue where filtering by tags on the Assets page would lead to an error.	01241243
Aligned the list of ignored plugins qualifying assets against the Tenable Security Center license with that of Tenable Vulnerability Management.	01219651

Corrected an issue when filters on the Vulnerability Analysis page would incorrectly be removed upon clearing values.	01220587
Correct a rare issue where asset information incorrectly displayed information from a different asset.	01219813
Corrected a formatting issue when creating a PDF that contained certain special characters.	01193789
A version check has been added so that the Tenable Security Center RPM can't be installed on the wrong OS version. An error message will be shown and the installation will stop if the user attempts to install on the wrong OS version.	N/A
Corrected an issue with Airwatch integration.	01123262
Deprecated "Network Type" has been removed from scan policy creation options.	01088164
Added optimizations when editing and deleting application-level Credentials, Audit Files, and Scan Policies to improve performance.	00711536
Corrected an issue where under certain circumstances Remediation Scans would error out.	00635591
Corrected a parsing issue in reports for the <> symbols.	00512200

Known Issues

- Log Correlation Engine Archived Silos cannot be selected in the Tenable Security Center UI

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.20.0.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.9.0 and later
OT Security	3.9.25 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.11.0 and later

Tenable Security Center Patch 202201.1 Release Notes (2022-01-12)

Note: This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running the following versions:

- Tenable Security Center 5.16.0 (CentOS 7 or RHEL 7)
- Tenable Security Center 5.16.1 (CentOS 7 or RHEL 7)
- Tenable Security Center 5.17.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.18.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.19.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.19.1 (CentOS 7, RHEL 7, CentOS 8, RHEL 8, or Oracle Linux 8)
- Tenable Security Center 5.19.1 (CentOS 7, RHEL 7, CentOS 8, RHEL 8, or Oracle Linux 8)

This patch updates Apache to version 2.4.52 and includes fixes for multiple Apache vulnerabilities: CVE-2021-44224 and CVE-2021-44790.

Tenable Security Center Version	Operating Systems
Tenable Security Center 5.16.0	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7)
Tenable Security Center 5.16.1	
Tenable Security Center 5.17.0	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7) • CentOS 8 • Red Hat Enterprise Linux 8 (RHEL 8)
Tenable Security Center 5.18.0	
Tenable Security Center 5.19.0	
Tenable Security Center 5.19.1	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7) • CentOS 8 • Red Hat Enterprise Linux 8 (RHEL 8) • Oracle Linux 8

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202201.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```
4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```
5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- bin/httpd

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 5.20.1 Release Notes (2022-01-24)

Note: Tenable recommends upgrading to the patch for this release, Tenable Security Center Patch 202204.1, which includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

Caution: If you are upgrading from Tenable Security Center 5.20.0 to Tenable Security Center 5.20.1 and you have overridden any Tenable-provided Asset Criticality Rating (ACR) values, do the following to upgrade to Tenable Security Center 5.20.1:

1. As the `tns` user, run the following command to perform a backup of `/opt/sc/hosts.db`:

   ```
   cp /opt/sc/hosts.db [backupfilename]
   ```

2. Upgrade to Tenable Security Center 5.20.1, as described in Upgrade Tenable Security Center in the *Tenable Security Center User Guide*.

3. After the upgrade completes, as the `tns` user, run the following command to restore `/opt/sc/hosts.db`:

   ```
   cp [backupfilename] /opt/sc/hosts.db
   ```

If you do not follow these upgrade steps, the Host Asset view page will be empty until the next scan import or until Tenable Security Center runs nightly jobs. Additionally, any overridden ACR values will reset to the Tenable-provided ACR values.

Important: When you upgrade from Tenable Security Center 5.20.0 to Tenable Security Center 5.20.1, the Host Assets view page will be appear to be blank until Tenable Security Center imports scan results or runs nightly jobs. Additionally, any overwritten Asset Criticality Rating (ACR) values will reset to the Tenable-provided ACR values.

If you want to keep your overwritten ACR values and ensure your Host Assets view page is populated immediately, use the following steps to upgrade to Tenable Security Center 5.20.1:

1. As the `tns` user, run the following command to perform a backup of `/opt/sc/hosts.db`:

   ```
   cp /opt/sc/hosts.db [backupfilename]
   ```

2. Upgrade to Tenable Security Center 5.20.1, as described in Upgrade Tenable Security Center in the *Tenable Security Center User Guide*.

3. After the upgrade completes, as the `tns` user, run the following command to restore your backup of `/opt/sc/hosts.db`:

   ```
   cp [backupfilename] /opt/sc/hosts.db
   ```

If you are running Tenable Security Center 5.12.0 or later, you can upgrade directly to Tenable Security Center 5.20.1. If you are running a version earlier than Tenable Security Center 5.12.0, upgrade to Tenable Security Center 5.12.0 before upgrading to Tenable Security Center 5.20.1.

If you are using Internet Explorer 11 on Windows 10 LTSB (build 14393.4104), you may need to add your Tenable Security Center installation to the “Trusted Sites” zone in order for the application to load.

If you are running Tenable Security Center 5.20.1 and you are using pyTenable with the Tenable Security Center API, you must upgrade pyTenable to version 1.4.2 or later.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.9.0 to 5.12.0 to 5.20.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Note: When you upgrade from Tenable Security Center 5.20.0 to Tenable Security Center 5.20.1, the Host Assets view page may be appear to be blank until Tenable Security Center runs nightly jobs.

Tenable Security Center Director

New Features

Asset Host View

Added a Host View table where you can see details about the asset, associated findings (vulnerabilities), and the associated software inventory.

For more information, see View Hosts in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

Bug Fixes

Bug Fix	Defect ID
The confidence level for the OS identification is now parsed from the plugin output, not just the operating-system-conf tag.	N/A
Corrected an issue with the sort order of IP addresses in the Host Assets view table.	N/A
Corrected an error when viewing CCE results on the Vulnerability Detail List page.	N/A
Fixed an issue that prevented SAML from working.	01323520 01323394
Fixed an issue where scans using an Advanced Scan Policy with the "Search for SSL/TLS services" option turned off under the Service Discovery tab would not function correctly.	01324016
Corrected an issue when using a cloud scanner with Tenable Security Center that under certain circumstances lead to incomplete results.	N/A
Resolved an issue on the Vulnerability Analysis page where the Output Asset Filter was removed when browsing Dashboard Component Data.	01220853
LCE Archive now selectable in user interface.	01330637
Corrected an issue with the display of plot points and trending lines.	01323667
Corrected an issue where the 192.168.x.x range was classified as an external address for ACR calculation purposes.	N/A
Corrected an issue that would lead to a scan import error under certain circumstances.	01326446
Corrected an issue that led to an error message when editing Windows credentials.	01324608

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.20.1.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.9.0 and later
OT Security	3.9.25 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.11.0 and later

Tenable Security Center Patch 202202.1 Release Notes (2022-02-01)

> **Note:** This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.20.0 and 5.20.1 on Red Hat EL 7, CentOS 7, Red Hat EL 8, and Oracle Linux 8. This patch fixes an error that can occur when importing scans (defect ID 01326446).

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202109.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- bin/agent_importdb
- bin/ipv4_importdb
- bin/ipv4_lce_importdb
- bin/ipv4_pvs_importdb
- bin/ipv6_importdb
- bin/ipv6_lce_importdb
- bin/ipv6_pvs_importdb

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202203.1 Release Notes (2022-03-03)

> **Note:** This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.20.0 or 5.20.1 on Red Hat EL 7, CentOS 7, Red Hat EL 8, and Oracle Linux 8. This patch updates scan processing to store the plugin output for all instances of the same vulnerability found on a single host.

SNIPPET ACROSS IO AND SC, DO NOT EDIT WITHOUT CONFIRMING CHANGES IN BOTH PRODUCTS

> **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

After applying the patch, plugin output shows each occurrence of the vulnerability along with its path, enabling a more granular approach for remediation workflows. All existing and future scans will take advantage of this updated capability the next time they run, without the need for additional configuration.

This update will not increase your vulnerability count for existing dashboards, reports, or Assurance Report Cards. Tenable Security Center will continue to count multiple instances of the same vulnerability on a host as a single vulnerability for reporting purposes.

> **Note:** This update may slightly increase the amount of data stored in your Tenable Security Center environment.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202109.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- ipv4_importdb
- ipv6_importdb
- agent_importdb
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202203.2 Release Notes (2022-03-09)

> **Note:** This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.20.0 or 5.20.1 on Red Hat EL 7, CentOS 7, Red Hat EL 8, and Oracle Linux 8. This patch corrects an issue introduced in Tenable Security Center 5.20.0 where the plugin output for certain compliance plugins contained invalid XML.

> **Note:** After you apply Tenable Security Center patch 202203.2, Tenable Security Center will report a PHP file integrity error until you upgrade Tenable Security Center to the next major version. This error is safe to ignore (the error only occurs because the patch replaces the VulnLib.php file).

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202109.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- VulnLib.php
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202204.1 Release Notes (2022-04-06)

> **Note:** This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.19.0, 5.19.1, 5.20.0, and 5.20.1. This patch updates Apache to version 2.4.53 and updates OpenSSL to version 1.1.1n to address the following vulnerabilities: CVE-2022-0778 and CVE-2022-23943.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202109.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- support/bin/httpd
- support/bin/openssl
- support/lib/libcrypto.so.1.1
- support/lib/libssl.so.1.1
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 5.23.1 Release Notes (2022-09-15)

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.12.0 or later, you can upgrade directly to Tenable Security Center 5.23.1. If you are running a version earlier than Tenable Security Center 5.12.0, upgrade to Tenable Security Center 5.12.0 before upgrading to Tenable Security Center 5.23.1.

If you are running Tenable Security Center 5.23.1 and you are using pyTenable with the Tenable Security Center API, you must upgrade pyTenable to version 1.4.2 or later.

If you upgrade Tenable Security Center Director, upgrade Tenable Security Center for all managed Tenable Security Center instances connected to Tenable Security Center Director. After upgrading, allow up to 15 minutes for your managed Tenable Security Center instances to sync with Tenable Security Center Director.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** If your upgrade path skips versions of Tenable Security Center (for example, upgrading from 5.9.0 to 5.12.0 to 5.23.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

> **Note:** Tenable Security Center 5.21.0 is the last version of Tenable Security Center that supports Internet Explorer. For more information about other supported browsers, see Web Browser Requirements in the *Tenable Security Center User Guide*.

New Features

Vuln Routing Rules

Tenable Security Center customers can route vulnerabilities to specific users with configurable filters.

For more information, see Vuln Routing Rules in the *Tenable Security Center User Guide*.

Nutanix Credential Integration

Tenable Security Center customers can now perform local, remote, and agent-based scans for their Nutanix AOS/AHV infrastructure.

For more information, see Miscellaneous Credentials in the *Tenable Security Center User Guide*.

Host Assets Export

Tenable Security Center customers can now export a list of hosts and their attributes on the **Host Assets** page.

For more information, see Export Hosts in the *Tenable Security Center User Guide*.

Asset Exposure Score (AES) Filtering

Tenable Security Center customers can now filter by AES and AES Severity on vulnerabilities, dashboards, and reports.

For more information, see Vulnerability Analysis Filter Components in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

Added commas to numbers with four or more digits to make them easier to read.

Bug Fixes

Bug Fix	Defect ID
Fixed a validation issue by adding a range validator to CVSS range input fields. The new validator will not allow users to enter an invalid value.	01450804
There was an issue with the backup/restore config tools related to compliance plugins. The config backup tool was modified to only get rows from the xref table in the plugins.db for distinct rowids. Previously the code was not doing this, resulting in a constraint error when trying to insert the rows on config restore.	01429824
Fixed an issue where Ticket Summary Dashboard components were incorrectly allowing the user to drill down, which led to an error in the UI.	01429302
Fixed an issue that caused an error when updating an existing user role.	01433817
Fix issue where certain Audit Files would not upload due to invalid file type.	01429636
Fixed a synchronization bug in the UI so that the frontend code waits for fetchRole operation to finish before doing any other FE operation.	01433037
Fixed an issue where scan results are inaccurate or getting removed on applying the Completion Time filter. Now when a user applies the Completion Time filter, Tenable Security Center returns all completed/finished scan results.	01431449

Fixed an issue where the Last Updated column was not sorting on the actual time of the column.	01429272
Fix missing plugin name when using vulnerability details list tools in a dashboard component.	01420121
Fixed an issue where the defragmentation job for repositories was being launched even in cases where it was not needed, causing other processes to take longer, like the preparation of remote repositories for synchronization.	01412532
An issue has been fixed in which adding an entry using a UUID format for the Hashicorp Vault Type for the Hashicorp Credential failed.	01405361, 01425261
Fixed the issue where system logs were not visible if the browser time zone was ahead of the Tenable Security Center server time zone.	01406784
Fixed an issue with user provisioning and Microsoft ADFS.	01360624
Vulnerability mitigation for the port scanner types of plugins - 14272, 14274, 34220 - are now considered to have a port scan of "all" for a particular host if they report any port for a scan for that host. This will now mitigate various ports that were found open in earlier scans that are now fixed, since these types of plugins scan all of the ports.	01374990
After a query has been deleted, users can now view, edit, export, or copy any report that references the deleted query. Now, owners of these reports can also move between groups.	01369194
Fixed a readability issue in the matrix cells by removing the alpha blending, so that it shows the background and text color.	01364070
Fixed an issue where sometimes one to all targets in a scan definition are scanned for, even inside an active Freeze Window.	01306531, 01378779
Role-based access control is now available for host assets. There is a new role, View Host Assets, to allow users to access host assets.	01327019
Fixed issues summing the number of devices in Asset Lists under repository contexts and across all repositories.	01287270
Fixed an issue where if a scanner that Tenable Security Center is utilizing for a	01287134

scan goes down and back up again, the original scan reports/chunks from that scanner are not cleaned up during the scan.	

Known Issues

- When a new user is created and the new user logs in right away after user creation, dashboards are not immediately populated with data.
- Switching quickly between LCE pages sometimes causes an error.
- There is an error when a user drills down into analysis pages, and then clicks the back button in the browser. The workaround is to navigate using the headers in Tenable Security Center.

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.23.1.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.9.0 and later
OT Security	3.9.25 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.11.0 and later

Tenable Security Center Patch 202209.2 Release Notes (2022-09-22)

Apply this patch to Tenable Security Center installations running Tenable Security Center 5.23.1. This patch fixes an issue where some users see an "invalid time value" error at login.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202109.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- html/index.html
- html/main.bf245dca013697ec9195.js

- html/runtime.3abecc10f9f301eed014.js
- html/vendors.b2f339cf84f31d23faea.js
- install.sh

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 2021

Tenable Security Center Patch 202102.2 Release Notes (2021-03-02)

Tenable Security Center Patch 202103.1 Release Notes (2021-03-15)

Tenable Security Center Patch 202104.1 Release Notes (2021-04-05)

Tenable Security Center Patch 202108.1 Release Notes (2021-09-01)

Tenable Security Center Patch 202109.1 Release Notes (2021-09-22)

Tenable Security Center 5.18.0 Release Notes (2021-04-01)

Tenable Security Center Q2 2021 Feed Update Release Notes (2021-07-22)

Tenable Security Center 5.19.0 Release Notes (2021-07-22)

Tenable Security Center 5.19.1 Release Notes (2021-09-01)

Tenable Security Center Patch 202110.1 Release Notes (2021-10-19)

Tenable Security Center Patch 202102.2 Release Notes (2021-03-02)

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running the following versions:

- Tenable Security Center 5.16.0 (CentOS 7 or RHEL 7 only)
- Tenable Security Center 5.16.1 (CentOS 7 or RHEL 7 only)
- Tenable Security Center 5.17.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)

This patch updates OpenSSL 1.1.1i to OpenSSL 1.1.1j to address the following CVEs: CVE-2021-23839, CVE-2021-23840 and CVE-2021-23841.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes. begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access in the *Tenable Appliance User Guide*. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.
2. Download the patch from https://www.tenable.com/downloads/tenable-sc to your Appliance. You can save the files in any location (e.g., `/tmp`).

3. Stop the Tenable Security Center instance from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.
4. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

5. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

6. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes.
7. Start Tenable Security Center from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.

Contents

- lib/libcrypto.so.1.1
- lib/libssl.so.1.1
- bin/openssl

Filenames and Checksums

Filenames and checksums are located on the Tenable Downloads page.

File	Product	MD5
SC-202001.2-5.13.0.tgz	Tenable Security Center on CentOS 6 Tenable Security Center on Red Hat Enterprise Linux 6.0 Tenable Security Center on CentOS 7	2ffb2feb521eb5b364ce7e5dc7b8e103

File	Product	MD5
	Tenable Security Center on Red Hat Enterprise Linux 7.0 Tenable Appliance 4.x	

Tenable Security Center Patch 202103.1 Release Notes (2021-03-15)

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running version 5.13.0 through 5.17.0.

This patch fixes a high risk Remote Code Execution vulnerability that allows an authenticated user to escalate privileges and gives them access to higher levels than intended within the Tenable Security Center console. The vulnerability exploits the Tenable Security Center server via Hypertext Preprocessor (PHP) unserialization.

This patch also fixes an issue that prevented Tenable Security Center from sending emails for Alerts.

> **Note:** This patch supersedes Tenable Security Center Patch 202102.1. Apply this patch to affected Tenable Security Center versions, even if you already applied Tenable Security Center Patch 202102.1.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file:

   ```
   tar zxf SC-202103.1-5.x.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes. begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- install.sh
- unserializePatch.php
- SerializeLib.php
- 5.13.0/AuthenticationLib.php
- 5.13.0/ConfigurationLib.php
- 5.14.0/AuthenticationLib.php
- 5.14.0/ConfigurationLib.php
- 5.14.1/AuthenticationLib.php
- 5.14.1/ConfigurationLib.php
- 5.14.1.1/AuthenticationLib.php
- 5.14.1.1/ConfigurationLib.php
- 5.15.0/AuthenticationLib.php
- 5.15.0/ConfigurationLib.php
- 5.16.0/AuthenticationLib.php

- 5.16.0/ConfigurationLib.php
- 5.16.0/importLCEVulns.php
- 5.16.0/importPVS.php
- 5.16.0/System.php
- 5.16.1/AuthenticationLib.php
- 5.16.1/ConfigurationLib.php
- 5.16.1/importLCEVulns.php
- 5.16.1/importPVS.php
- 5.16.1/System.php
- 5.17.0/AuthenticationLib.php
- 5.17.0/ConfigurationLib.php
- 5.17.0/importLCEVulns.php
- 5.17.0/importPVS.php
- 5.17.0/System.php

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202104.1 Release Notes (2021-04-05)

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running the following versions:

- Tenable Security Center 5.16.0 (CentOS 7 or RHEL 7 only)
- Tenable Security Center 5.16.1 (CentOS 7 or RHEL 7 only)
- Tenable Security Center 5.17.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)

This patch updates OpenSSL 1.1.1j to OpenSSL 1.1.1k to address CVE-2021-3449.the following CVEs: CVE-2021-3449 and CVE-2021-3450.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file:

   ```
   tar zxf SC-202104.1-5.x.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes. begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- lib/libcrypto.so.1.1
- lib/libssl.so.1.1
- bin/openssl

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202108.1 Release Notes (2021-09-01)

> **Note:** This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running the following versions:

- Tenable Security Center 5.17.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.18.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)

This patch updates OpenSSL 1.1.1j to OpenSSL 1.1.1k to address CVE-2021-3449.the following CVEs: CVE-2021-3449 and CVE-2021-3450.

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file:

   ```
   tar zxf SC-202108.1-5.x.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes. begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- lib/libcrypto.so.1.1
- lib/libssl.so.1.1
- bin/openssl
- bin/php
- modules/libphp7.so
- bin/sqlite3
- lib/libsqlite3.so.0.8.6
- html/index.html
- html/main.js
- html/vendors.js

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center Patch 202109.1 Release Notes (2021-09-22)

> **Note:** This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running the following versions:

- Tenable Security Center 5.16.0 (CentOS 7 or RHEL 7)
- Tenable Security Center 5.16.1 (CentOS 7 or RHEL 7)
- Tenable Security Center 5.17.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.18.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)

- Tenable Security Center 5.19.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.19.1 (CentOS 7, RHEL 7, CentOS 8, RHEL 8, or Oracle Linux 8)

Tenable Security Center Version	Operating Systems
Tenable Security Center 5.16.0	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7)
Tenable Security Center 5.16.1	
Tenable Security Center 5.17.0	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7) • CentOS 8 • Red Hat Enterprise Linux 8 (RHEL 8)
Tenable Security Center 5.18.0	
Tenable Security Center 5.19.0	
Tenable Security Center 5.19.1	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7) • CentOS 8 • Red Hat Enterprise Linux 8 (RHEL 8) • Oracle Linux 8

This patch updates OpenSSL 1.1.1k to OpenSSL 1.1.1l to address following CVEs:

- CVE-2021-3711 — Fixed in OpenSSL 1.1.1l (affected 1.1.1-1.1.1k)
- CVE-2021-3712 — Fixed in OpenSSL 1.1.1l (affected 1.1.1-1.1.1k)

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.
3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202109.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- lib/libcrypto.so.1.1
- lib/libssl.so.1.1
- bin/openssl

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 5.18.0 Release Notes (2021-04-01)

> **Tip:** Tenable rebranded SecurityCenter as Tenable Security Center. For more information, see the announcement.

> **Note:** Tenable recommends upgrading to the patches for this release, Tenable Security Center Patch 202108.1, Tenable Security Center Patch 202109.1, Tenable Security Center Patch 202110.1, and Tenable Security Center Patch 202201.1, which include fixes for potential vulnerabilities. For more information, see the Tenable Product Security Advisory.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** This release includes fixes from Tenable Security Center Patch 202103.1.

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.9.0 or later, you can upgrade directly to Tenable Security Center 5.18.0. If you are running a version earlier than Tenable Security Center 5.9.0, upgrade to Tenable Security Center 5.9.0 before upgrading to Tenable Security Center 5.18.0.

If you are using Internet Explorer 11 on Windows 10 LTSB (build 14393.4104), you may need to add your Tenable Security Center installation to the “Trusted Sites” zone in order for the application to load.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

This release includes an upgrade to OpenSSL 1.1.1k. This resolves two issues found in the open source libraries, CVE-2021-3450 and CVE-2021-3449. Both issues were rated High.

> **Note:** If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.9.0 to 5.18.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

> **Note:** On April 30, 2021, Tenable Nessus versions 8.5.1 and earlier (including Tenable Nessus Professional and managed scanners) will reach End of Standard Support. On May 1, 2021, scanners running Tenable Nessus versions 8.5.1 and earlier will still be able to run scans, but they will not receive plugin updates.
>
> If you upgrade to Tenable Security Center 5.18.0:
>
> - Managed scanners running Tenable Nessus versions 8.5.2 or later will continue to receive plugin updates and perform scans as usual.
> - Managed scanners running Tenable Nessus versions 8.5.1 and earlier will no longer be able to perform scans. All scanners will need to be upgraded to Tenable Nessus version 8.5.2 or later.
>
> For more information, see the knowledge base article.

> **Note:** As part of an ongoing diversity and inclusion effort, Tenable is updating language to align with industry standards for inclusive language. Tenable Security Center 5.18.0 will support both the Blackout Window and Freeze Window API. In Tenable Security Center 5.19.0, the Blackout Window API call will be deprecated and will only support the Freeze Window API. The functionality of the API will remain the same.

Tenable Security Center Director

New Features

Tenable Nessus Scanner and Scan Zone Management in Tenable Security Center Director

Added the ability for Tenable Security Center Director administrators to add, edit, and delete Tenable Nessus scanners and scan zones on managed Tenable Security Center instances.

For more information, see Nessus Scanners and Scan Zones in the *Tenable Security Center Director User Guide*.

LDAP User Provisioning

Added the ability to automatically create LDAP-authenticated users in Tenable Security Center by importing user account attributes from your Microsoft Active Directory. When user provisioning is enabled, users who log into your Active Directory are automatically created in Tenable Security Center. Active Directory user passwords are never stored in Tenable Security Center.

This feature has been tested with Microsoft Server 2016 Active Directory on-premises and Microsoft Server 2019 Active Directory on-premises (not Azure Active Directory).

For more information, see LDAP User Provisioning in the *Tenable Security Center User Guide*.

Data Expiration at Repository Level

Added the ability to set data expiration at a repository level. There will no longer be a global setting for data expiration. When upgrading to Tenable Security Center 5.18.0, repositories inherit the data expiration settings based on your previous global settings.

For more information, see Agent Repositories and IPv4/IPv6 Repositories in the *Tenable Security Center User Guide*.

New Export Option for Solution Details

Added the ability to export the fields on the Solution Details page as a `.csv` file.

For more information, see Export Hosts Affected by a Solution in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

- When you export vulnerabilities as a `.csv` file, the column labeled "Plugin Text" has been changed to "Plugin Output."
- The minimum required version for Java has been updated from Java 1.4 to Java 1.8.

Bug Fixes

Bug Fix	Defect ID
Added logic to roll back any changes made in connection with Log Correlation Engine data updates should there be an error.	1086533
Fixed a bug in trend lines where data imported close to the snapshot time was not being included in the numbers for each day when using the "First Observed"	1122068

and "Last Observed" filters.	
Fixed a bug where sorting was not being preserved on list views when moving back and forth on different pages.	586959
Fixed a bug with PDF reports generating incorrect values for the iterator when Tenable Security Center finds multiple assets assigned with the same UUID.	1115183
Fixed a bug within the Vulnerability Analysis view where the value that was being preserved for sorting is a column that does not exist for the tool.	
Fixed a memory allocation error in the list software tool that somewhat infrequently causes the tool to crash.	
Fixes a defect in Scan Results where user may have seen "No Values" as options for Group filter on slower connections.	785460
When a user signs in and there is an unassigned certificate available, the user will presented with a new dialogue. If the user selects "Yes", the certificate will assigned to that user and they will be logged in immediately, skipping the "Change Password" dialogue if that option was set for the user.	1019727
Resolved an issue where a Class A or B or C summary in Vulnerability Analysis could not properly export IP addresses into a CSV Report.	1153755
Resolved an issue where Internet Explorer 11 did not properly render fonts when using Tenable Security Center.	951822
Resolved an issue where the drill down of certain matrix cells with default clauses would improperly navigate to the Vulnerability Summary page, instead of the Vulnerability List page.	1110694
Resolved an issue where exceedingly rare cases the Job Daemon could crash when it fails to read the Application database.	1172455
Tenable Security Center customers on CentOS 8 with SELinux enforcing who are using Log Correlation Engine need to allow rsync to run ssh by changing the rync_client value: setsebool -P rsync_client 1	
Scanners and Groups with the same name will be renamed as duplicates to ensure these tables have unique naming in the future.	

Tenable Security Center now validates port scan ranges to ensure they meet the requirements for scans using Tenable Vulnerability Management and Tenable Nessus scanners. Invalid ranges will now cause errors at scan time in Tenable Security Center instead of on the scanners mid-scan.	830350
The code has been modified so that the first user created in an organization (userID == 1) cannot be deleted.	559685
Fixed a problem when Tenable Security Center couldn't login to a scanner and treated it as failed. At that point Tenable Security Center reinjected the chunks from the scanner that went offline. However Tenable Security Center was reinjecting chunks that had already been downloaded and marked as complete. This caused Tenable Security Center to scan some of the hosts twice and caused Tenable Security Center to stop before all the hosts had been scanned. Fixed to only reinject chunks that are not completed.	1091012
Objects belonging to one user in a group fails to migrate properly when a User is deleted with their objects being shared to another group. Admin and Organization users can now migrate a user's objects without errors upon that user's deletion.	1091273
Working files created during feed update are deleted after the feed update completes. This resolves a problem in which the files were not deleted, eventually filling the disk.	1090063
Alerts : Emails are not received with Email action and getting error log in the sc-error.log file	
Find/Update Filters - Shows "undefined"	1157589
If you link the Tenable Vulnerability Management cloud scanner using password only and launch an agent scan with duration set to 1 day it will throw an error. The message erroneously reported the ID of the Agent Scan being ran instead of the ID of the Scanner.	1146658
When migrating from any earlier version of Tenable Security Center to Tenable Security Center 5.17.0, any existing Database Credentials (in that they existed before the migration) will erroneously have their sybase_ase_auth_type field set to "RSA". This field is only meant for Sybase Database credential types and not	1148242

all Database credential types so the Credential Validator trips up on this. For more information, see the knowledge base article.	
Agent Capable Scanner is not showing up within the Agent Scanner drop down.	1141081
Fixed a Vulnerability Queries segment fault that occurs in a rare use case.	1131863
"User's group does not have access to xxxxx Repository" message hovering over repo.	1124963
Analysis View Shows Total, but Page says "No Results Found."	1088995
Fixed an issue with the Query Tool for reports. When you select a Query for a report, the fields in the Definition section are populated based on the query definition. If the user changes one of those fields, the Query field is supposed to be cleared. When you select a Query, and then modify the filters (add a new one, delete one, or edit an existing one), the Query field is cleared. The same thing should happen if the user selects a different Tool.	1105118
Agent Group Name Change Not Reflected in Web UI.	1083510
Fixed the Content-Security-Policy header in the Tenable UI directive to the correct value.	
Fixed a rounding error in the scan completion duration.	1037558
Fixed Trending Repo Date Range Max Limit of 365 During Quick Setup (max limit should be 999).	1028110
Rename "Scan Policy Plugins" Filter on Active Scans/Results Pages to "Scan Policy."	984313
Vulnerability Analysis not clearing filter in UI.	752877
Remove Purge Tickets from Workflow Permissions Role View.	713105
In Vuln Analysis clicking 'IP Summary' from the 'DNS Name Summary' tool links incorrectly to events.	629975

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.18.0.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.5.1 and later
OT Security	3.4.9 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.9.0 and later

Tenable Security Center Q2 2021 Feed Update Release Notes (2021-07-22)

Tenable Security Center released the following feed updates during Q2 2021. To take advantage of these updates on any supported version of Tenable Security Center, do one of the following:

- Configure recurring automatic feed updates for the Tenable Security Center feed, as described in Edit Plugin and Feed Settings and Schedules in the (missing or bad snippet).
- Perform an offline Tenable Security Center feed update, as described in Perform an Offline Tenable.sc Feed Update in the (missing or bad snippet).

New Features

New and Updated Dashboards and Reports

Tenable Security Center Report Templates

- Qatar 2022 Cybersecurity Framework Executive Summary Report
- CIS Linux and Unix Benchmark Reports
- 2020 Threat Landscape Retrospective Report
- Microsoft Exchange Server ProxyLogon/Hafnium Detection Report
- CIS Microsoft Workstations Benchmark Reports
- NIA Operations Summary Report

Tenable Security Center Dashboards

- Windows Patch Level/Rollup Tracking
- Database One-Stop-Shop
- Operations Dashboard
- Tracking Microsoft Security Bulletins Dashboards
- Qatar 2022 Cybersecurity Data Protection Dashboard
- Microsoft Exchange Server ProxyLogon/Hafnium Detection Dashboard
- InfoSec Team – One-Stop Shop Comprehensive Attack Surface
- Cyber Risk Executive Briefing
- Worst of the Worst - Fix These First!
- Qatar 2022 Cybersecurity Framework Network Security
- Qatar 2022 Cybersecurity Framework Executive Summary
- Qatar 2022 Cybersecurity Framework Endpoint Security
- Qatar 2022 Cybersecurity Framework Application Security
- Qatar 2022 Cybersecurity Change and Patch Management Dashboard
- Qatar 2022 Cybersecurity Operations Technology Security Monitoring Dashboard
- CIS Audit Summary

- CIS Control 11: Secure Network Devices
- 2020 Threat Landscape Retrospective
- CNBV – User and Access Management

Assurance Report Cards

- Tracking NIA Asset Classification

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Tenable Security Center 5.19.0 Release Notes (2021-07-22)

> **Note:** Tenable recommends upgrading to the following patches for this release, which include fixes for potential vulnerabilities:
>
> - Tenable Security Center Patch 202109.1
> - Tenable Security Center Patch 202110.1
> - Tenable Security Center Patch 202201.1
> - Tenable Security Center Patch 202204.1
>
> For more information, see the Tenable Product Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.9.0 or later, you can upgrade directly to Tenable Security Center 5.19.0. If you are running a version earlier than Tenable Security Center 5.9.0, upgrade to Tenable Security Center 5.9.0 before upgrading to Tenable Security Center 5.19.0.

If you are using Internet Explorer 11 on Windows 10 LTSB (build 14393.4104), you may need to add your Tenable Security Center installation to the “Trusted Sites” zone in order for the application to load.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

Note: This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.9.0 to 5.19.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Tenable Security Center Director

New Features

Dark Mode

Added the ability to view Tenable Security Center in dark mode.

For more information, see User Accounts in the *Tenable Security Center User Guide*.

Increased Repository Size

Upgraded the maximum repository size from 32GB to 64GB and added the ability to view repository capacity.

For more information, see Repositories in the *Tenable Security Center User Guide*.

Write-Ahead Logging (WAL) Mode

Added the ability to enable write-ahead logging to reduce issues with database locks.

For more information, see Tenable Security Center Database Journaling Modes in the *Tenable Security Center User Guide*.

Database backup in support of WAL

In support of the Write Ahead Logging (WAL) feature we have added support for database backup of the metadata related to WAL.

Tenable Security Center-Tenable Lumin Synchronization Support for Overlapping IP Addresses

Added the ability to synchronize Tenable Security Center repositories to individual networks in Tenable Vulnerability Management instead of synchronizing all repositories to the default Tenable Vulnerability Management network.

For more information, see Lumin Synchronization in the *Tenable Security Center User Guide*.

Tenable Security Center Director License Allocation Dashboard Widget

Added a widget to the Tenable Security Center Director Insights dashboard that shows license usage across multiple Tenable Security Center instances.

For more information, see Insights Dashboard in the *Tenable Security Center Director User Guide*.

View System Logs for Managed Tenable Security Center Instances

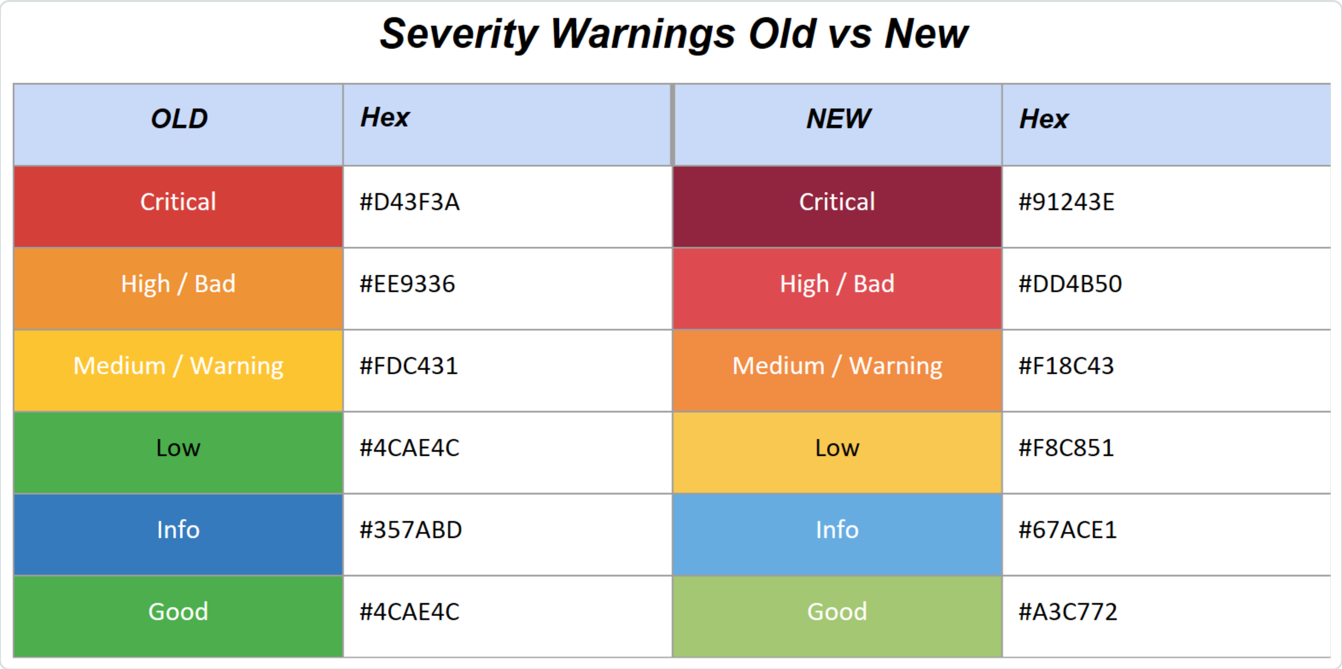
Added the ability to view all managed Tenable Security Center instance system logs from a centralized Tenable Security Center Director.

For more information, see System Logs in the *Tenable Security Center Director User Guide*.

UI Improvements

To give our users a more updated and consistent experience across Tenable products we have made the following changes:

- Improved appearance of Tenable Security Center buttons, filters, and other elements in some areas of the UI, including dashboards, vulnerability analysis, user roles, and reports.
- Updated the colors for severity messages



Severity Warnings Old vs New

OLD	Hex	NEW	Hex
Critical	#D43F3A	Critical	#91243E
High / Bad	#EE9336	High / Bad	#DD4B50
Medium / Warning	#FDC431	Medium / Warning	#F18C43
Low	#4CAE4C	Low	#F8C851
Info	#357ABD	Info	#67ACE1
Good	#4CAE4C	Good	#A3C772

Generic SSH Compliance Checks

Added the ability to perform generic SSH checks regardless of underlying platform.

For more information about compliance scan policy options, see Compliance Options in the *Tenable Security Center User Guide*.

ZTE Plugin Support

Added the option for ZTE Plugin for audits.

For more information about compliance scan policy options, see Compliance Options in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

- Removed support for RTF reports in Tenable Security Center. Existing RTF report jobs will be automatically converted to PDF. Existing RTF reports will be preserved.
- Because Shibboleth 1.3 SSO has reached end of life, Tenable Security Center has added a message to warn users that Shibboleth 1.3 will no longer be supported with the next release.

  > **Note:** To avoid future upgrade errors, Tenable recommends updating to Shibboleth 2.0.

- Added support for privilege escalation for Arcon SSH credentials.
- Upgraded to PHP 7.4

Bug Fixes

Bug Fix	Defect ID
Fixed count in the List OS view. The count in the List OS view is different than when you drill down on an entry and check the total results. Some of the counts were correct but others were not.	00572284
Fixed a permission issue relating to a failed check for DISA Red Hat Linux 6 STIG Version 1 Release 18.	00592555
Fixed an issue whereby vulns do not mitigate on certain ports for agent scans as well as active scans. Also, understanding of "default" ports and "all" ports now fits with that of Tenable Nessus.	N/A
Resolved a "Max Sessions Error Occurring" in rare situations where sessions counts weren't tracked correctly.	00689916

Fixed an issue where dashboard components on the same schedule did not always line up visually. (e.g. Matrix columns, in particular)	00692279
Security Managers will be able to see notifications for feed updates that they initiated	00702290
Resolved a divide by zero error in a metric that can occur in a custom report.	00709655
Fixed information missing in report after renaming.	00778031
Fixed job errors related to an already deleted report	00772175
Resolved an issue with accuracy in Scan results	00801204
Scans will now show a status message "Import Pending" when the scan has completed, but the import has not yet started.	00869302
Fixed issue in Vulnerability Analysis where "Name" sort sorts by Plugin ID incorrectly	00977750
Fixed issue when create report using cumulative data setting is ignored	00999725
Fixed issues where agent-sync scan in Tenable Security Center returns incorrect count when previewing and importing	00990365
The reported error message has been modified to reflect that it is not related to Session Management. This will now report "Your Tenable Security Center session token is invalid or has expired. Please login and try again." Customers who see the original error frequently may continue to see it due to connectivity, storage, or other such limitations.	01021135
Fixed an issue when set to more than 120 days, scan results show in the “Scan Results" tab. But then the screen is stuck there, unable to navigate to a screen such as "Active Scans."	01026145
When editing a policy, toggling a preference that causes other preferences to become hidden will reset those preferences to their default value in the saved policy definition.	01044449
Fixed a database issue encountering malformed database disk image in jobqueue.db	01045650

Fixed "Validation failure" while generating a CSV or PDF from scan results	01059340
Fixed reports generating with an odd separation between IP and results	01068033
The user when creating a CSV report had plugin output data that the code was processing incorrectly and splitting the data within the plugin output in such a way that other fields were getting corrupted causing the CSV file to contain jumbled data. The code was modified to not split the plugin output data resulting in a correctly formatted CSV file.	01116654
Fixed maximum character limit for CVE-ID query parameter that caused report to fail	01130071
Fixed an issue where exported policies from a simplified Chinese locale Tenable Security Center lose settings detail.	01139041
Resolved an issue where an upgrade of Tenable Security Center could incorrectly fail with an insufficient disk space error.	01147796
Resolved an issue where all plugin types were not displaying in dashboard.	01149389
Code was added to nightly cleanup that handles stale schedule objects such that if the owner of a schedule object has been deleted, the schedule object is removed from the schedule.	00679875
Fixed a cross-reference filter that returns no results against remote repositories.	01154865
Removed the call to rm.js as that file no longer exists.	01158192
Resolved an error where a linked user account was unable to view system logs	01159707
Fixed a bug where VPR scores were getting lost for plugins. A Tenable Security Center feed update adds the VPR scores and context for plugins. A plugin update after that (active or passive) was clearing the VPR score (not the VPR context). The plugin update code was modified (for both active and passive plugins) so that the VPR scores are maintained.	01158300
Addressed rare interaction between simultaneous Tenable Security Center scans.	01162312

Fixed an issue with audit files not being able to be utilized in ASR reports.	01163544
Fixed API documentation error regarding parameters sent to dnsName.	01167364
Fixed an issue where a user was unable to import scan into Tenable Security Center, in spite of repository covering the IP range of all targets included in the scan	01173874
Fixed an issue were a terminated user is still showing on reports under the shared section	01148195
Resolved an issue where "/rest/configSection/0" API call was returning empty key/value pair ("features":{"":""})	01172378
Fixed an issue where the Initiator filter was not applying in the system logs view	01177778
Fixed an issue where plugins including 145071, 146060 & 146948 were not displayed after initial scan in remediation scans or subsequent scans.	01176974, 01171369
Fixed an issue where plugin name was not being displayed in the vulnerability detailed view in dashboards	01174465
Resolved an issue where Accept Risk repo filter was not working.	01177668
Fixed an issue where LDAP integration forced username/password after a Tenable Security Center upgrade	01191763
Fixed an issue where "invalid port_range preference" errors would occur under certain conditions.	01192043
Fixed an issue where in rare circumstances a "too many arguments" error would be generated when performing a command line upgrade	01193926
Fixed an issue where under certain circumstances PHP warnings for dns_get_record would write multiple entries to the log	01185071
Resolved the issue with under Group Permissions in Add Users where more than 5 Groups are not showing with the scrollbar.	01194924
Fixed an issue where if an API user did not log into the Tenable Security Center UI the account would lock out after a certain period of time	01196404

Fixed an issue where the Vulnerability Mitigated filter (if selected) would be removed from CSV reports when saving	01192147
Fixed an issue where Remediation scan was showing up incorrectly in the settings when a vulnerability was selected in an Agent repository.	N/A
Fixed an issue where authsources-custom.php was not migrated to the updated location after upgrading Tenable Security Center	01199001
Fixed an issue of "uncaught type" error message appearing when hovering over the membership group info icon	01196049
Fixed an issue where under certain circumstances a self signed certificate would fail to generate after upgrading from an older (<5.16) version of Tenable Security Center	01197421
Fixed an issue where in the Scanners screen where the Tenable Nessus Scanner Version column was not sorting correctly	01199316
Fixed an issue introduced in Tenable Security Center 5.18 where the Output Assets filter was not working correctly	01202395
Fixed an issue where under certain circumstances attempting to view the version of Java using the command line would return an error	01201749
Fixed a rare error when scans would not import correctly when using a sequence of characters preceding a '\'	01188621
Fixed an issue with error handling when sending an incorrectly formatted SAML request	01199951
Fixed a display issue with the "Load Query" dialog box appearing off screen	01209052
Fixed an issue where under certain circumstances filter pop-up windows would not display correctly on the Vulnerability Analysis screen	01200001
Resolved an issue where the IP address is overwriting after uploading both the `.nessus` files in one repository with "Scan Virtual hosts" ON	01210833

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.19.0.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version
Tenable Nessus	8.5.1 and later
OT Security	3.4.9 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.9.0 and later

Tenable Security Center 5.19.1 Release Notes (2021-09-01)

> **Note:** Tenable recommends upgrading to the following patches for this release, which include fixes for potential vulnerabilities:
>
> - Tenable Security Center Patch 202109.1
> - Tenable Security Center Patch 202110.1
> - Tenable Security Center Patch 202201.1
> - Tenable Security Center Patch 202204.1
>
> For more information, see the Tenable Product Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

Tenable Security Center 5.19.1 adds support for Oracle Linux 8, adds the option to use credentials for MongoDB scanning, and resolves an issue where the **Scan Virtual Hosts** option occasionally prevented mitigation of that data.

> **Note:** This is not a mandatory release. Tenable recommends upgrading to 5.19.1 only if you need support for any of the previously listed scenarios. All of these changes will be included in the next Tenable Security Center release alongside other new capabilities.

Upgrade Notes

If you are running Tenable Security Center 5.9.0 or later, you can upgrade directly to Tenable Security Center 5.19.1. If you are running a version earlier than Tenable Security Center 5.9.0, upgrade to Tenable Security Center 5.9.0 before upgrading to Tenable Security Center 5.19.1.

If you are using Internet Explorer 11 on Windows 10 LTSB (build 14393.4104), you may need to add your Tenable Security Center installation to the "Trusted Sites" zone in order for the application to load.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** This release includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

> **Note:** If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.9.0 to 5.19.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Tenable Security Center Director

New Features

MongoDB Database Credentials

Added the ability to scan a MongoDB database with a username, password, and port number.

For more information, see Database Credentials in the *Tenable Security Center User Guide*.

Oracle Linux 8 Support

Added support for OracleLinux 8 (RedHat compatible kernel only) as an alternative to CentOS 8, which RedHat announced will go end of life on December 31, 2021. Tenable Security Center will continue to support CentOS 7, RHEL 7, and RHEL 8.

For more information about Tenable Security Center system requirements, see System Requirements in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

-

Bug Fixes

Bug Fix	Defect ID
Updated the list of ignored plugins qualifying assets against the Tenable Security Center license with that of Tenable Vulnerability Management.	01219651
Fixed an issue where the **Scan Virtual Hosts** option was causing data to sometimes be stored in a way that prevented mitigation of that data.	01171216

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.19.1.

For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Product	Tested Version

Tenable Nessus	8.5.1 and later
OT Security	3.4.9 and later
Tenable Log Correlation Engine	6.0.0 and later
Tenable Network Monitor	5.9.0 and later

Tenable Security Center Patch 202110.1 Release Notes (2021-10-19)

Note: This release includes fixes for vulnerabilities. For more information, see the Tenable Product Security Advisory.

Apply this patch to Tenable Security Center installations running version 5.16.0 or later. This patch includes fixes for multiple Apache vulnerabilities: This patch updates from Apache 2.4.48 to version 2.4.51 to address CVE-2021-33193, CVE-2021-34798, and CVE-2021-40438.

- Tenable Security Center 5.16.0 (CentOS 7 or RHEL 7)
- Tenable Security Center 5.16.1 (CentOS 7 or RHEL 7)
- Tenable Security Center 5.17.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.18.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.19.0 (CentOS 7, RHEL 7, CentOS 8, or RHEL 8)
- Tenable Security Center 5.19.1 (CentOS 7, RHEL 7, CentOS 8, RHEL 8, or Oracle Linux 8)

Tenable Security Center Version	Operating Systems
Tenable Security Center 5.16.0	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7)
Tenable Security Center 5.16.1	

Tenable Security Center Version	Operating Systems
Tenable Security Center 5.17.0	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7) • CentOS 8 • Red Hat Enterprise Linux 8 (RHEL 8)
Tenable Security Center 5.18.0	
Tenable Security Center 5.19.0	
Tenable Security Center 5.19.1	• CentOS 7 • Red Hat Enterprise Linux 7 (RHEL 7) • CentOS 8 • Red Hat Enterprise Linux 8 (RHEL 8) • Oracle Linux 8

Steps to Apply

Apply the patch to a standalone Tenable Security Center or Tenable Core + Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.

3. Run the following command to untar the patch file, where [*patch file name*] is the name of the .tgz patch file you downloaded:

   ```
   tar zxf SC-202109.1-5.x.tgz
   ```

   ```
   tar zxf [patch file name]
   ```

4. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory created in step 3:

   ```
   cd [directory]
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

What to do next:

- (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the knowledge base article.

Contents

- bin/httpd

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Security Center 2020

Tenable Security Center Patch 202001.1 Release Notes (2020-01-07)

Tenable Security Center Patch 202001.2 Release Notes (2020-01-08)

Tenable Security Center Patch 202004.1 Release Notes (2020-05-05)

Tenable Security Center 5.14.1 Release Notes (2020-04-20)

Tenable Security Center 5.15.0 Release Notes (2020-07-16)

[Tenable Security Center 5.16.0 Release Notes (2020-10-06)]

[Tenable Security Center 5.17.0 Release Notes (2020-12-21)]

Tenable Security Center Patch 202001.1 Release Notes (2020-01-07)

Apply this patch to Tenable Security Center installations running version 5.9.x, 5.10.x, 5.11.x, or 5.12.x. This patch updates SimpleSAMLPHP to version 1.17.7.

For more information, see the Security Advisory.

Contents

- saml/ folder

Steps to Apply

Apply the patch to your Tenable Security Center or Tenable Appliance deployment.

Apply the patch to a standalone Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access in the *Tenable Appliance User Guide*. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.

2. Download the patch from https://www.tenable.com/downloads/tenable-sc to your Appliance. You can save the files in any location (e.g., `/tmp`).

3. Stop the Tenable Security Center instance from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.

4. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

5. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

6. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes.

7. Start Tenable Security Center from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.

Filenames and MD5 Checksums

File	Product	MD5
SC-202001.1-5.x.tgz	Tenable Security Center on CentOS 6 Tenable Security Center on Red Hat Enterprise Linux 6.0 Tenable Security Center on CentOS 7 Tenable Security Center on Red Hat	64f408bbcf168317e0a58147fbf7709a

File	Product	MD5
	Enterprise Linux 7.0 Tenable Appliance 4.x	

Tenable Security Center Patch 202001.2 Release Notes (2020-01-08)

Apply this patch to Tenable Security Center installations running version 5.13.0. This patch includes updates to address an integration issue with ServiceNow.

Contents

- VulnLib

Steps to Apply

Apply the patch to your Tenable Security Center or Tenable Appliance deployment.

Apply the patch to a standalone Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access in the *Tenable Appliance User Guide*. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.
2. Download the patch from https://www.tenable.com/downloads/tenable-sc to your Appliance. You can save the files in any location (e.g., `/tmp`).
3. Stop the Tenable Security Center instance from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.
4. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

5. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

6. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes.
7. Start Tenable Security Center from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.

Filenames and MD5 Checksums

File	Product	MD5
SC-202001.2-5.13.0.tgz	Tenable Security Center on CentOS 6 Tenable Security Center on Red Hat Enterprise Linux 6.0 Tenable Security Center on CentOS 7 Tenable Security Center on Red Hat	`2ffb2feb521eb5b364ce7e5dc7b8e103`

File	Product	MD5
	Enterprise Linux 7.0 Tenable Appliance 4.x	

Tenable Security Center Patch 202004.1 Release Notes (2020-05-05)

Apply this patch to Tenable Security Center installations running version 5.14.1. This patch resolves an issue in Tenable Security Center 5.14.1 where attempting to generate a debug file with the **Strip IPs** option enabled would result in an error.

Contents

- FilesystemLib

Steps to Apply

Apply the patch to your Tenable Security Center, Tenable Core, or Tenable Appliance deployment.

Apply the patch to a standalone Tenable Security Center or Tenable Core:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes. begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access in the *Tenable Appliance User Guide*. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.
2. Download the patch from https://www.tenable.com/downloads/tenable-sc to your Appliance. You can save the files in any location (e.g., `/tmp`).
3. Stop the Tenable Security Center instance from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.
4. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

5. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

6. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes.
7. Start Tenable Security Center from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.

Filenames and Checksums

Filenames and checksums are located on the Tenable Downloads page.

File	Product	MD5
SC-202001.2-5.13.0.tgz	Tenable Security Center on CentOS 6 Tenable Security Center on Red Hat Enterprise Linux 6.0 Tenable Security Center on CentOS 7	`2ffb2feb521eb5b364ce7e5dc7b8e103`

File	Product	MD5
	Tenable Security Center on Red Hat Enterprise Linux 7.0 Tenable Appliance 4.x	

Tenable Security Center 5.14.1 Release Notes (2020-04-20)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tip: Tenable rebranded SecurityCenter as Tenable Security Center. For more information, see the announcement.

Note: Tenable recommends upgrading to the patch for this release, Tenable Security Center Patch 202102.1Tenable Security Center Patch 202103.1, which includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

Tenable Security Center 5.14.1 is a replacement for Tenable Security Center 5.14.0 to resolve an issue during upgrade and an issue on the **Lumin Status** page. After reviewing the Upgrade Notes, you can download the update files from the Tenable Security Center Downloads page.

This release addresses multiple third-party vulnerabilities. For more information, see the Security Advisory.

Upgrade Notes

This release fixes a migration issue that appeared in the Tenable Security Center 5.14.0 release related to an SQL unique ID constraint. You can upgrade to Tenable Security Center 5.14.1 following the normal process if you successfully upgraded to Tenable Security Center 5.14.0 or if you never attempted to upgrade to Tenable Security Center 5.14.0.

If you attempted to upgrade to Tenable Security Center 5.14.0 but you received error messages of any kind (for example, an error message that included `....SQL-STATE[HY000]: General error: 1 no such column:...`), contact Tenable Support for assistance upgrading to Tenable Security Center 5.14.1.

Upgrade Path

If you are running version Tenable Security Center 5.6.2.1 or later, you can upgrade directly to version 5.14.1. If you are running a version earlier than 5.6.2.1, upgrade to version 5.6.2.1 before upgrading to version 5.14.1.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.14.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

New Features

Hashicorp Vault PAM Integration

Added support for the use of Hashicorp Vault PAM SSH, Windows, and database credentials in active scans.

For more information, see SSH Credentials, Windows Credentials, and Database Credentials Authentication Method Settings in the *Tenable Security Center User Guide*.

Arcon PAM Integration

Added support for the use of Arcon PAM SSH and Windows credentials in active scans.

For more information, see SSH Credentials and Windows Credentials in the *Tenable Security Center User Guide*.

SAML Metadata Import

Admin users can now upload their identity provider metadata into Tenable Security Center’s SAML configuration instead of manually entering the details.

For more information, see Configure SAML Authentication Automatically via the Tenable Security Center Interface in the *Tenable Security Center User Guide*.

Performance Improvements

Improved performance for the following processes: asset import and preparation, queries, and repository snapshots.

Tenable Security Center to Lumin Connector

Tenable Security Center now supports dynamic assets tags in addition to static asset tags.

An automatic sync feature has been added for asset tags. When asset tag information is updated in Tenable Security Center, the new version automatically syncs to Lumin once per day.

For more information, see Configure Lumin Synchronization in the *Tenable Security Center User Guide*.

The new Lumin Data feature displays the latest values for Cyber Exposure Score, Assessment Maturity Grade, and other log details of the transfer of data to Lumin. This will help the user know when sync data has been completed and help monitor changes in Lumin metrics.

For more information, see Lumin Data in the *Tenable Security Center User Guide*.

Bug Fixes

Bug Fix	Defect ID
Tenable Security Center 5.14.0 upgrade bug when two or more scanners had the same name.	N/A
Resolved an issue in displaying metrics on the Lumin Status page when configured with a proxy. This did not impact synchronization functionality.	N/A
Resolved an issue when viewing Recast Rules, where filtered state wasn't preserved when using the back-button	444720
Resolved an issue that displayed from deleted users as "Administrator", and prevented the user from being able to resolve or close them	461859
Resolved an issue where dashboards were unnecessarily re-evaluated after editing the tab layout	798659
Resolved an issue where an Asset names would occasionally get duplicated in vulnerability analysis filters	604512
Resolved an issue where explicit date filters on the Report Results page did not work as expected	622511
Resolved an issue in System Logs where the initiator filters for admins were not working as expected	633191
Resolved an issue where diagnostic scans would log password information when failing under limited scenarios	674476

Resolved an issue where generating a diagnostic debug zip file could error from utilizing too much memory.	714863
Resolved an issue editing scans that targeted Assets that had since been deleted	721349
Resolved a issue with viewing trend data in the Event Analysis page when using some versions of Internet Explorer	734485
Resolved an issue where reports would show break ("<br/>") characters in limited scenarios	747220
Resolved an issue preventing filtering on Agent Repositories in the Accept / Recast Risk pages	749275
Resolved an issue on the plugins page where explicit time filters were not working properly	753436
Resolved an issue where a sort column in a report could not be modified	765963
Resolved an issue where Asset preparation jobs could fail when using specific clause types	766331
Resolved an issue where the usage of offsets in the /analysis/download API did not work as expected	N/A
Resolved an issue where Agent Scans could not be modified in some scenarios	797592
Fixed an issue in custom Dashboards where the "Mitigated On" Field was sometimes not properly populated with the correct data.	805401
Resolved an issue where Audit File Template types were duplicated when modifying a Scan Policy	810130
Resolved an issue where some date filters were not working as expected when using the "Send to report" option on a dashboard	828391
Resolved an issue where alert actions assigned to yourself were not working as expected.	875558
Resolved issue in Vulnerability Analysis where asset information for an IP Address was sometimes not displayed correctly	880012

Resolved issue where plugin remediation/solutions for Skype/Lync applications were not working properly	889540
Resolved an issue where users could not be edited after transitioning from authentication type LDAP to Certification.	893631
Resolved an issue when sorting by VPR and using the sumid tool	902748
Resolved an issue where the search feature for Zones while editing Scans was not working as-expected in certain scenarios	909368
Resolved an issue where post-scan reports with special characters in their names did not work properly	908856
Resolved an issue impacting synchronization to Lumin when using a proxy setup.	950960
Resolved an issue that prevented the ability to view agent Assets in some scenarios.	957659
Resolved an issue where the Date column in the System Logs page was improperly appearing as sortable	N/A
Resolved an issue where dashboards would sometimes erroneously show extremely large numbers for trending on vulnerability counts.	962583
Resolved an issue where the default display columns in the Vulnerability Analysis page for the IP Summary tool did not include DNS and NetBIOS	N/A
Resolved an issue where Alert "Actions" were not marked as a required field on the Alerts page	N/A
Resolved an issue where the notification message after adding a custom plugin was displaying as "Undefined Added Successfully"	N/A
Resolved an issue on the Repositories page where the type-sort functionality was not working properly for all repository types	N/A
Resolved an issue where proper email addresses did not pass validation in the Distribution section of a Report	N/A
Resolved an issue where the Password field was not indicated as mandatory in	N/A

the UI when editing an Industrial Security Instance	
Resolved an issue when sorting by type on the Policies page	N/A
Resolved an issue where Feed Updates would continue to show as Updating after they had completed	N/A
Resolved an issue where PHP notices were generated in the logs for CSV reports with no display columns	N/A
Resolved an issue where the log would note an invalid error after adding or updating a license / activation code	N/A
Resolved an issue where the title of the Solutions page was displaying the non-descriptive title: "Tenable.sc"	N/A
Resolved an issue where Alerts improperly allowed all Actions to be removed on edit	N/A
Resolved an issue where a misleading error would appear in the logs after attempting to add an invalid activation code on the License Configuration page	N/A
Resolved an issue where a job didn't effectively terminate, and could theoretically grow over time.	N/A
Resolved issue where the notification message on dashboard delete would display as: "Dashboard unshared successfully"	N/A
Resolved an issue where PHP notices would appear in the logs after an Active Plugin update	N/A
Resolved an issue where the drilldown of certain matrix cells with default clauses would improperly navigate to the Vulnerability Summary page, instead of the Vulnerability List page	N/A
Resolved an issue where PHP warnings (relating to "runScore") could appear in the logs when syncing data to Lumin	N/A
Resolves an issue that impacted ServiceNow integration functionality. This is the same issue resolved in the "Tenable Security Center 5.13.0 ServiceNow Patch"	N/A
Resolved an issue where the Debug Options toggles would not show as disabled	N/A

while downloading logs for a Nessus Scanner	
Reduced the severity of VPR Plugin update log messages to more accurately reflect meaning	N/A

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.14.1:

Product	Tested Version
Nessus	8.5.1 and later
Log Correlation Engine	5.1.1 and later
Nessus Network Monitor	5.9.0 and later
Industrial Security	1.4.0 and later
OT Security	3.4.9 and later

Tenable Security Center 5.15.0 Release Notes (2020-07-16)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tip: Tenable rebranded SecurityCenter as Tenable Security Center. For more information, see the announcement.

> **Note:** Tenable recommends upgrading to the patch for this release, Tenable Security Center Patch 202102.1Tenable Security Center Patch 202103.1, which includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

For information about security updates included in this release, see the Security Advisory.

Upgrade Notes

If you are running Tenable Security Center 5.6.2.1 or later, you can upgrade directly to Tenable Security Center 5.15.0. If you are running a version earlier than Tenable Security Center 5.6.2.1, upgrade to Tenable Security Center 5.6.2.1 before upgrading to Tenable Security Center 5.15.0.

If you are running Tenable Security Center 5.11.0, 5.12.0, or 5.13.0, upgrade to Tenable Security Center 5.14.1 before upgrading to Tenable Security Center 5.15.0 to avoid a potential migration issue.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.15.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

New Features

Migration Enhancements

The following updates reduce errors during Tenable Security Center upgrades and assist with troubleshooting upgrade issues:

- Added alerts for issues with file permissions and ownership, available disk space, and available PHP memory.
- Added command line error messages for errors that occur during upgrade.
- Improved procedural logging and error handling for failures that occur during upgrade.

Nessus Agent Scan Scheduling through Tenable Security Center

Users in Tenable Security Center can now configure, schedule, and launch basic agent scans in Tenable Security Center that run on a linked Tenable Nessus Manager. When the agent scan completes, results are imported to an agent repository in Tenable Security Center.

For more information about agent scanning in Tenable Security Center, see Agent Scanning in the *Tenable Security Center User Guide*.

Note: Agent scans configured before upgrading to Tenable Security Center 5.15.0 are called agent synchronization jobs in Tenable Security Center 5.15.0 and later. For more information, see Agent Synchronization Jobs in the *Tenable Security Center User Guide*.

Bug Fixes

Bug Fix	Defect ID
Remediated a condition during asset calculations causing it to hang.	01011947
Import scan bug that in rare occurrences will fail due to db lock issue.	01021386
The option to export a remote repository was available when it should not have been present.	N/A
The user could still update their plugins when an inactive product code was present. Resolved by checking when an inactive code is detected and disabling the corresponding feed update button.	N/A
Plugin/Feed update does not display error when configured without activation code.	N/A
When the cross-reference (xref) field is processed by the plugin parser, ensure the application checks for the proper delimiter before parsing the data.	N/A
Data not retained as expected after DHCP change where IPs on 2 hosts are swapped.	N/A
Resolves an issue where touch debugging was not being generated for Resolve Host Names.	N/A
Any time a scan result is imported into a Tenable Security Center repository that is synchronized to Tenable Vulnerability Management/Lumin, synchronization data is displayed when viewing the scan result.	N/A

Synchronization data will no longer be displayed for Tenable Security Center repositories that are not synchronized to Tenable Vulnerability Management/Lumin.	
Fixes bug where running diagnostics with Scrub IPs turned on will break Tenable Security Center debug zip creation.	N/A
Fixes a bug with the Tenable Security Center scan feature that takes an unresponsive scanner out of service correctly, but does not resend the proper policy payload to re-initiate the scan when the scanner becomes active.	N/A
Fixed an issue where settings could change when importing or exporting policies.	N/A
This bug fix adds two new filters to the VPR, CVSS v2, and CVSSv3 filters on Vulnerability Analysis: "None" and "All." This will now allow for a customer to search by "None" to display vulns with no score, "All" with every vuln (with and without a score), and finally the ability to search by a range. The default for this is "All."	N/A
This fixes a bug that when an upgrade occurs, the `/etc/pki/tls/certs` directory is changed to the `tns` user. Now the `/etc/pki/tls/certs` directory owner will no longer be modified for upgrades of Tenable Security Center.	N/A
Fixed an issue where "List Software" was not showing for Debian/Ubuntu even when 22869 has results.	N/A
The “Search for SSL/TLS on” setting in Scan Policies contains an option for a user to set the Service Discovery Options. Even when the setting was hidden and turned off, exporting the policy would turn the value on. The fix will ensure that if the setting is off prior to the export, the setting will remain off after the export is complete.	N/A
Fixed an issue causing excessive memory usage in the vulnerability-querying sub-system that powers Dashboards, Analysis, Reporting, and ARCs.	01023338

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.15.0.

Product	Tested Version
Nessus	8.5.1 and later
OT Security	3.4.9 and later
Log Correlation Engine	5.1.1 and later
Nessus Network Monitor	5.9.0 and later

Tenable Security Center 5.16.0 Release Notes (2020-10-06)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tip: Tenable rebranded SecurityCenter as Tenable Security Center. For more information, see the announcement.

Note: Tenable recommends upgrading to the following patches for this release, which include fixes for potential vulnerabilities:

- Tenable Security Center Patch 202102.2
- Tenable Security Center Patch 202103.1
- Tenable Security Center Patch 202104.1
- Tenable Security Center Patch 202109.1

- Tenable Security Center Patch 202110.1
- Tenable Security Center Patch 202201.1

For more information, see the Tenable Product Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

Upgrade Notes

If you are running Tenable Security Center 5.6.2.1 or later, you can upgrade directly to Tenable Security Center 5.16.0. If you are running a version earlier than Tenable Security Center 5.6.2.1, upgrade to Tenable Security Center 5.6.2.1 before upgrading to Tenable Security Center 5.16.0.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.16.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

New Features

Linked Users

This feature introduces the ability for a Tenable Security Center administrator to log in with credentials once and switch to a different user without having to enter credentials again. The first time a user logs in, they must log in as an administrator. The user can then create additional linked users tied to their administrator account. Each linked user is a Security Manager in the Full Access group. Linked user accounts can only be accessed by the user logging into their admin account first; you cannot directly log in to a linked user account. All login activity is logged for full audit reporting.

For more information, see Linked Users in the *Tenable Security Center User Guide*.

Enhanced Tenable Security Center to Tenable Lumin Connector Status Information

This feature provides the following enhancements to the Tenable Security Center to Tenable Lumin Connector:

- Tenable Lumin Data Metrics: The metrics on the Tenable Lumin Data page are now computed nightly for faster data retrieval. Metrics are preserved on the Tenable Lumin Data page until they are computed again.
- Tenable Lumin Dashboard Link: On the Tenable Lumin data page, a link is now provided that opens the Tenable Lumin dashboard in a separate browser tab so that the user can quickly view all Lumin metrics.
- Tenable Lumin History Log: The History Log on the Tenable Lumin Data page now includes the transfer duration for assets in addition to repositories.
- Test Connection Button: The Tenable Lumin Configuration page now has a button for testing the connection to Tenable Vulnerability Management and Tenable Lumin. After pressing the button, a message is displayed providing the following information:
  - The connection was successful.
  - The connection was unsuccessful.
  - The connection was successful, but the IO container license has expired.
  - The connection was successful, but Lumin is not enabled.
  - The connection was successful, but the Lumin license has expired.

For more information, see Configure Lumin Synchronization, View Lumin Data Synchronization Logs, and View Lumin Metrics in the *Tenable Security Center User Guide*.

Tenable Vulnerability Management Agent Scan Scheduling through Tenable Security Center

Users in Tenable Security Center can now configure, schedule, and launch basic agent scans in Tenable Security Center that are run through a linked Tenable Vulnerability Management instance. When the agent scan completes, results are imported to an agent repository in Tenable Security Center.

For more information about agent scanning in Tenable Security Center, see Agent Scanning in the *Tenable Security Center User Guide*.

SAML User Provisioning

Tenable Security Center can now be configured to create and modify users automatically from either a SAML 2.0 or Shibboleth 1.3-based identity provier.

For more information, see SAML Authentication in the *Tenable Security Center User Guide*.

Hashicorp Vault Integration

Added support for Hashicorp Vault Active Directory, Key/Values 1, and Key/Values 2 secrets engines.

For more information, see SSH Credentials, Windows Credentials, and Database Credentials Authentication Method Settings in the *Tenable Security Center User Guide*.

IBM DataPower Gateway Integration

Added support for IBM DataPower Gateway credentials.

For more information, see API Gateway Credentials in the *Tenable Security Center User Guide*.

Changed Functionality and Performance Enhancements

- Removed the ability to provide a password when using the Import method for Oracle Database credentials. For more information, see Database Credentials in the *Tenable Security Center User Guide*.
- You can now only perform user/password bulk imports via the API. For more information, see Credential in the *Tenable Security Center API Guide*.

Bug Fixes

Bug Fix	Defect ID
Fixes memory minor memory leaking for the "List Vuln" and "Vuln Detail" tools. Reduced memory usage for the "Vulnerability Summary" tool during most cases when not VPR sorting. Fixes known segfault bug while sorting on VPR score for "Vulnerability Summary" tool.	
Fixed an issue with displaying IPv6 addresses on the vulnerability details of agent repositories.	
For customers using Tenable Core + Tenable Security Center, upgrades of Tenable Security Center were failing due to an error in calculating the amount of free disk space available for the upgrade.	01062912
Fixed an issue with incorrect results being returned while browsing individual scan results and using vulnerability text filtering.	01080513

Fixed an issue where the "Server Calculation error" icon displayed instead of "loading" icon for policy statement after adding the ARC template.	
Fixed an issue where Stop button was incorrectly displayed on Agent Scan.	
Fixed an issue where deleting users from large user sets could halt Tenable Security Center operations for a short time.	
Fixed an issue where users could not publish report results from the gear dropdown menu on the report result list view.	
Fixed a longstanding bug where Intune MDM credentials were causing mobile repository syncs to fail.	
Fixed an issue where an incorrect confirmation message would be displayed for deleting a dashboard component.	
Fixed an issue where VPR and CVSS score was not displaying decimals.	
Fixed an issue where the expiration for accepted risk rules did not take into account accept risk rules for agent repositories.	
Fixed an issue where the Tenable UUID was not migrating with DHCP tracking for IPv4 repositories.	
Fixed an issue where running a remediation scan against a Windows target caused an accurately displayed NetBios name to change to “Unknown."	
Fixed an SQL error that occurs during upgrade from Tenable Security Center 5.11.0, 5.12.0, or 5.13.0 to Tenable Security Center 5.15.0 (skipping Tenable Security Center 5.14.1) if the customer has duplicate users in their database.	01061736

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.16.0.

Product	Tested Version
Tenable Nessus	8.5.1 and later
OT Security	3.4.9 and later
Tenable Log Correlation Engine	5.1.1 and later
Tenable Network Monitor	5.9.0 and later

Tenable Security Center 5.17.0 Release Notes (2020-12-21)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tip: Tenable rebranded SecurityCenter as Tenable Security Center. For more information, see the announcement.

Note: Tenable recommends upgrading to the following patches for this release, which include fixes for potential vulnerabilities:

- Tenable Security Center Patch 202102.2
- Tenable Security Center Patch 202103.1
- Tenable Security Center Patch 202104.1
- Tenable Security Center Patch 202108.1
- Tenable Security Center Patch 202109.1
- Tenable Security Center Patch 202110.1
- Tenable Security Center Patch 202201.1

For more information, see the Tenable Product Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

Note: CentOS 6 and RHEL 6 are end of life and are not supported on Tenable Security Center 5.17 and later.

Upgrade Notes

If you are running Tenable Security Center 5.9.0 or later, you can upgrade directly to Tenable Security Center 5.17.0. If you are running a version earlier than Tenable Security Center 5.9.0, upgrade to Tenable Security Center 5.9.0 before upgrading to Tenable Security Center 5.17.0.

If you are using Internet Explorer 11 on Windows 10 LTSB (build 14393.4104), you may need to add your Tenable Security Center installation to the “Trusted Sites” zone in order for the application to load.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

> **Note:** If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.9.0 to 5.17.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Tenable Security Center Director

In this new section of the release notes, we will be detailing all new functionality for Tenable Security Center Director. Tenable Security Center Director is available as an add-on to Tenable Security Center and Tenable Security Center Continuous View customers. It provides a single pane of glass to view and manage customers' entire vulnerability landscape, across multiple consoles. Providing centralized management and data insight, Tenable Security Center Director puts more data at customer’s fingertips to ensure complete visibility across their network. For more information regarding this product please visit the Tenable Security Center product page.

New Features

CVSS v2/v3 Support

Provided ability for customers to manage severity based on CVSS rating version 2 or version 3 at an organizational level. Recast Rules work as before, taking precedence over CVSS score. When a user changes the CVSS version, the results will be immediate. Trend dashboards will display historical data based on the CVSS version configured at the time the data was calculated. For example, if there is 30 days worth of trend data and the administrator changes from CVSS v2 to v3, the 30 days of trend data will remain as-is. Only new data would be calculated using CVSS v3.

User Feedback

Users on consoles with Usage Statistics Enabled will see a new question mark icon on the top of each page. Clicking this will bring up a feedback form that users can use to provide feedback about the product. Please note that this form is not for bug or feature request creation. All feedback will be sent directly to Tenable to be reviewed.

Sybase DB

Added support for Sybase database credentials.

For more information, see Database Credentials in the *Tenable Security Center User Guide*.

Centrify PAM

Added the ability to use Centrify to lookup passwords for Windows and Linux machines.

For more information, see SSH Credentials and Windows Credentials in the *Tenable Security Center User Guide*.

Thycotic Secret Server Privilege Escalation

Added support for Thycotic Secret Server privilege escalation for SSH credentials.

For more information, see SSH Credentials and Privilege Escalation in the *Tenable Security Center User Guide*.

Bug Fixes

Bug Fix	Defect ID
Fixed three minor bugs with Database Debugging: Database locks debugging is now working for import, prepareassets and the showvulns binaries. Timestamps for those binaries now also align to the PHP time zone setting. Syslogging those binaries is now implemented and is accomplished through the same settings. (No changes to the UI.)	
Fixes a query error on Analysis page when the Vulnerability Details tool is used.	
Fixed an issue that generated an error when locking/unlocking a linked user account	
Fixed an issue where Severity Summary for Vulnerability Analysis was sometimes reporting incorrect results or crashing.	

Fix an issue on scan import where host information is incorrectly duplicated for a single host resulting in erroneous analysis (Realtime, Dashboard, ARC and Reporting, etc.) as well as data exported to Lumin (via the Lumin connector) to be incorrect.	
Fixed an issue where sometimes parsing an uploaded Nessus file, especially from Tenable Vulnerability Management, fails to import and is stored as a malformed file on Tenable Security Center.	1119932
Fixed cross reference information for Red Hat Security Advisory plugins to report the Bulletin ID and link to the article.	1102988
Fixed missing NetBIOS name from a diagnostic scan of an asset.	1072126
Fixed an issue with setting a trend line to end at some point in the future, or having an installation with a time zone that is ahead of UTC time, which causes a gap in presentation of data at the front of the trend line.	1036057
Fixed an issue where in some cases .nessus files were unable to be imported into Tenable Security Center	00975711
Fixed an issue where exporting individual scan results as a PDF were causing an error	00631075
Removed invalid MSFT reference links	00589977
Fixed an issue where the Vulnerability Analysis page would display incorrect system information	00740415
Fixed an issue with the Agent scan preview filter button	00884965
Fixed an issue around SAML login failures after upgrading from 5.14.1	
Fixed a timezone bug displaying Istanbul as GMT+2 and Turkey permanently on GMT+3	00987630
Fixed an issue on the Class B Summary view	00803913
Fixed an issue with the /user endpoint returning erroneous data	00809520
Fixed an error resulting from searching for a specific section and then selecting the vulnerability analysis section	01030913

Fixed an issue with scan policies not saving more than two vCenter passwords	01009565
Fixed an issue with the /analysis vuln type requests not working correctly	00763099
Fixed an issue with mismatched tags on some manual .nessus imports	01119932
Fixed an issue using the type filter for events	01023774
Fixed an issue with incorrect system information displaying on individual scan results	01059432

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and Checksums

Filenames and MD5 or SHA-256 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.17.0.

Product	Tested Version

Tenable Nessus	8.5.1 and later
OT Security	3.4.9 and later
Tenable Log Correlation Engine	5.1.1 and later
Tenable Network Monitor	5.9.0 and later

2019 Tenable Security Center

2019 Tenable Security Center

Tenable Security Center 2019

Tenable Security Center Patch 201906.1 Release Notes (2019-06-25)

Apply this patch to Tenable Security Center installations running version 5.10.1 only. You do not need to apply this patch to Tenable Security Center installations running earlier versions. The fixes in this patch resolve an issue with the multi-showids tool.

Contents

- multi-showids

Steps to Apply

Apply the patch to your Tenable Security Center or Tenable Appliance deployment.

Apply the patch to a standalone Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access in the *Tenable Appliance User Guide*. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.

2. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

```
sh ./install.sh
```

The installation runs and finishes.

Filenames and MD5 Checksums

File	Product	MD5
SC-201906.1-5.10.1-rh6-64.tgz	Tenable Security Center 5.10.1 on CentOS 6 Tenable Security Center 5.10.1 on Red Hat Enterprise Linux 6.0 Tenable Appliance 4.x	ce952c71040896e6c3cc390d2c0b3797

Tenable Security Center Patch 201911.2 Release Notes (2019-11-12)

Apply this patch to Tenable Security Center installations running version 5.7.x, 5.8.x, 5.9.x, 5.10.x or 5.11.x. This patch updates PHP to version 7.1.33 to address CVE-2019-13224 and resolves issues with the SC-201911.1 patch.

For more information, see the Security Advisory.

Contents

- libphp7.so
- php

Steps to Apply

Apply the patch to your Tenable Security Center or Tenable Appliance deployment.

Apply the patch to a standalone Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and Tenable Security Center is stopped. After the installation finishes, Tenable Security Center automatically restarts.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access in the *Tenable Appliance User Guide*. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.

2. Download the patch from https://www.tenable.com/downloads/tenable-sc to Tenable Security Center. You can save the files in any location (e.g., `/tmp`).

3. Stop the Tenable Security Center instance from Appliance, as described in Manage Tenable Security Center in the *Tenable Appliance User Guide*.

4. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

5. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

6. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

The installation runs and finishes.

7. Start Tenable Security Center from Appliance, as described in [Manage Tenable Security Center](#) in the *Tenable Appliance User Guide*.

Filenames and MD5 Checksums

File	Product	MD5
`SC-201911.2-5.x-rh6-64.tgz`	Tenable Security Center 5.7.x, 5.8.x, 5.9.x, 5.10.x or 5.11.x on CentOS 6 Tenable Security Center 5.7.x, 5.8.x, 5.9.x, 5.10.x or 5.11.x on Red Hat Enterprise Linux 6.0 Tenable Appliance 4.x	`aef50c6f103418f77d0bfef93f9aaf2d`
`SC-201911.2-5.x-rh7-64.tgz`	Tenable Security Center 5.7.x, 5.8.x, 5.9.x, 5.10.x or 5.11.x on CentOS 7 Tenable Security Center 5.7.x, 5.8.x, 5.9.x, 5.10.x or 5.11.x on Red Hat Enterprise Linux 7.0	`df168e632f6fd35ecfd4852b0e16a464`

Tenable Security Center 5.10.0 Release Notes (2019-05-06)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle [Matrix](#) and [Policy](#).

If you are running version 5.6.2.1 or later, you can upgrade directly to version 5.10.0. If you are running a version earlier than 5.6.2.1, upgrade to version 5.6.2.1 before upgrading to version 5.10.0.

> **Note:** If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.7.0 to 5.10.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

You can download the update files from the Tenable Security Center Downloads page.

New Features

VPR Key Drivers

Additional fields have been added to the Vulnerability Detail List view to give a better understanding of the Vulnerability Priority Rating (VPR) Score:

- Vulnerability Age
- CVSS v3 Impact Score
- Exploit Code Maturity
- Product Coverage
- Threat Intensity
- Threat Recency
- Threat Sources

For more information, see View Vulnerability Instance Details in the *Tenable Security Center User Guide*.

Touch Debugging

While logged in as Admin, under System / Diagnostics, users now have the ability to enable Touch Debugging through the UI, reducing time and complexity of providing debug logs to Tenable Support.

For more information, see Diagnostics in the *Tenable Security Center User Guide*.

Rebranding

Additional rebranding to "Tenable.sc" has been completed in this release.

Enhanced Telemetry

Tenable Security Center is moving to an "Opt-out" policy for returning anonymized usage statistics. This option can be found while logged in as Admin under the Miscellaneous Configuration section.

For more information, see Privacy Configuration Settings in the *Tenable Security Center User Guide*.

API Key Support

Tenable Security Center has moved from Security Certificates to utilizing API keys for data transfer. This has the benefit of removing certificate timeout issues.

For more information, see Nessus Scanners in the *Tenable Security Center User Guide*.

Suspend/Resume Scans

For more information, see Suspend or Resume a Scheduled Active Scan in the *Tenable Security Center User Guide*.

IP Randomization

Enabling this setting will cause Tenable Security Center to send randomized blocks of IPs to Nessus scanners. This can be enabled while logged in as Admin under the Miscellaneous Configuration page.

For more information, see Scanning Configuration Settings in the *Tenable Security Center User Guide*.

Bug Fixes

Bug Fix	Defect ID
In order to enhance product security, the following configuration file changes have been made on initial install: • "Strict-Transport-Security" header • "Content-Security-Policy" header • "X-Content-Type-Options" header • "X-XSS-Protection" header • Update SSL Cipher suite • Prevent TLS 1.0 and TLS 1.1 from being used	00511314

• Make sure cookies have the SameSite flag enabled	
Fixed an issue where Passive Plugins were missing their VPR Score.	n/a
OpenSSL has been upgraded to version 1.0.2r.	n/a
Fixed an issue where creating an Advanced Assurance Report Card without any base filters would cause unneeded error logging.	n/a
Fixed an issue where incorrectly parsed plugins were causing incorrect CVSS V2 Vector results to be produced.	00776841
Fixed an issue where "System name" was being sent as an empty string when sending Lieberman credentials	00688244
Fixed an issue where users were unable to sort using the repository column when using the IP summary tool	00768144
Fixed an issue where importing agent data into IP repository would get stuck in a pending state	00768587
Fixed a Glibc error "Scan import error (code 11)" when importing specific scan results	00762804
Fixed an issue where in some cases, jobs, scheduled by specifying the day of the week in recurrence, generated errors and did not launch as expected.	00766085
Fixed an issue where plugin #34220 was failing to remediate from an agent scan	00752612
Fixed an issue where Agent Malware Scan could remove previous DNS entries from a repository	00742128
Fixed an issue where new assets could fail to calculate	00720889
Fixed an issue where exporting report templates that were share across multiple groups could result in a timeout error	00725421
Fixed an error where the name of a custom audit file would not be displayed	00663634
Fixed an issue when Agent sync to Tenable Security Center could result in an Unauthorized (401) error	00619991

Fixed an issue where Plugin search shows "show IP details" pop up instead of "show plugin details" pop up	00715839

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Guide.

Filenames and MD5 Checksums

Filenames and MD5 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.10.0:

Product	Tested Version
Nessus	6.3.0 and later
Nessus Manager	7.1.0 and later
Log Correlation Engine	5.0.6 and later
Nessus Network Monitor	5.1.1 and later
3D Tool	2.0 and later

Tenable Security Center 5.10.1 Release Notes (2019-06-19)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tip: Tenable rebranded SecurityCenter as Tenable Security Center. For more information, see the announcement.

If you are running version 5.6.2.1 or later, you can upgrade directly to version 5.10.1. If you are running a version earlier than 5.6.2.1, upgrade to version 5.6.2.1 before upgrading to version 5.10.1.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.10.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

You can download the update files from the Tenable Security Center Downloads page.

Bug Fixes

Bug Fix	Defect ID
Resolved issue where the "CyberArk Escalation Account Details Name" field was not functioning properly.	00761670
Resolved an issue in the Tenable Security Center plugin feed that was causing database locking issues.	00806742
Resolved an issue where start up banners did not work correctly for certificate-authenticated users.	00810188
Resolved an issue where start up banners did not work correctly for certificate-authenticated users.	00810109

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Guide.

Filenames and MD5 Checksums

Filenames and MD5 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.10.1:

Product	Tested Version
Nessus	8.5.1 and later
Log Correlation Engine	5.1.1 and later

Nessus Network Monitor	5.9.0 and later
Industrial Security	1.4.0 and later

Tenable Security Center 5.11.0 Release Notes (2019-07-29)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tip: Tenable rebranded SecurityCenter as Tenable Security Center. For more information, see the announcement.

If you are running version 5.6.2.1 or later, you can upgrade directly to version 5.11.0 If you are running a version earlier than 5.6.2.1, upgrade to version 5.6.2.1 before upgrading to version 5.11.0.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.11.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

You can download the update files from the Tenable Security Center Downloads page.

New Features

Group Preference for Sample Content

This setting allows customers to choose whether a group will receive a default set of objects for users in the group. You can disable this option to reduce undesired content for performance and overhead concerns.

For more information, see Groups in the *Tenable Security Center User Guide*.

VPR Sorting

You can now sort by VPR in dashboards, reports, and on the Vulnerability Analysis page.

Increased Password Security

Tenable Security Center updated existing password storage logic to use a SHA512 hash and use PBKDF2 for increased security and FIPS compliance.

For more information, see Encryption Strength in the *Tenable Security Center User Guide*.

Security-Enhanced Linux (SELinux) Support

Tenable Security Center now supports enforcing mode for the Linux kernel security module, SELinux.

For more information, see System Requirements in the *Tenable Security Center User Guide*.

Scan ID in reports

Reports generated from scan results now include relevant scan information on the cover page.

For more information, see Report Options in the *Tenable Security Center User Guide*.

Feed Refresh

The following audit files are now supported: F5, Acatel Lucent TiMOS devices, and NetApp 9.

For more information, see Add a Template-Based Audit File in the *Tenable Security Center User Guide*.

Bug Fixes

Bug Fix	Defect ID
Resolved several issues to reduce database locking.	n/a
An issue with BeyondTrust integration 401 errors has been resolved.	00778027
Miscellaneous warnings have been cleaned up.	n/a
Resolved an issue where Vulnerability Analysis view counts did not include all vulnerabilities for very large repositories.	n/a
Minor fixes for log file formatting / wording.	n/a
Resolved an issue where creating a scan with an incorrect date format could cause system instability.	00841517
Resolved an issue where you could not use the Event Analysis views if you installed Tenable Security Center on RHEL 6.	00828770
Resolved an issue where an admin was unable to add an LDAP user when SAML is enabled.	00809428
Resolved an issue where an Organization's Accept Risk Rules and Recast Risk Rules were not being properly cleaned up when the organization was being	00806638

deleted.	
Resolved an issue where BeyondTrust Credentials were not being recognized by Tenable Security Center.	00778027
Resolved an issue causing remote repositories to fail synchronization.	00773719
Fixed an issue where failed credentials to a given host were mitigating remote check vulnerabilities detected locally.	00765334
Resolved an issue where the Diagnostics page System Status incorrectly reported Java version 10 or later as unsupported.	00758526
Resolved an issue where Industrial Security debug information was not properly being displayed in the logs.	00761607
Resolved an issue where Tenable Security Center would incorrectly parse IPv4 addresses from imported .nessus files.	00691735
Resolved an issue where Plugin Family Filters was not filtering correctly.	00692598
Resolved upgrade issues around SAML.	00834761
Resolved an issue that prevented LCE information from being queried in Analysis.	00828770
Resolved potential 500 errors when accessing alerts.	00808440

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and MD5 Checksums

Filenames and MD5 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.11.0:

Product	Tested Version
Nessus	8.5.1 and later
Log Correlation Engine	5.1.1 and later
Nessus Network Monitor	5.9.0 and later
Industrial Security	1.4.0 and later

Tenable Security Center 5.12.0 Release Notes (2019-10-03)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

If you are running version 5.6.2.1 or later, you can upgrade directly to version 5.12.0 If you are running a version earlier than 5.6.2.1, upgrade to version 5.6.2.1 before upgrading to version 5.12.0.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.12.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

You can download the update files from the Tenable Security Center Downloads page.

New Features

Privileged Account Auditing

Tenable Security Center now logs additional events for auditing administrator accounts:

- User lock / user unlock
- User create / user edit / user delete
- Enable password complexity / disable password complexity
- Changing maximum number of login attempts
- Changing the login banner
- Changing session management settings
- Changing login notification settings

- Changing any field within data expiration
- Changing header text

Admin License Component

You can now view an **Overview Dashboard** graph of your license usage over time in relation to your current license maximum.

For more information, see Overview Dashboard in the *Tenable Security Center User Guide*.

Nessus Log Retrieval

You can now download Nessus logs directly from Tenable Security Center.

For more information, see Download Nessus Scanner Logs in the *Tenable Security Center User Guide*.

Nessus Health Status

Tenable Security Center now displays Nessus health information to assist in troubleshooting.

For more information, see View Nessus Scanner Details in the *Tenable Security Center User Guide*.

Tenable Security Center Health Status Fields

Tenable Security Center now displays additional health checks on the existing Tenable Security Center **Diagnostics** page.

For more information, see Diagnostics in the *Tenable Security Center User Guide*.

Solutions View

This new view allows you to better assess your Cyber Exposure and focus on the most important actions first.

For more information, see View Solutions in the *Tenable Security Center User Guide*.

Disable PHP Serialization

You can now disable export functionality in Tenable Security Center (e.g., dashboard export, report export, etc.).

For more information, see Security Settings in the *Tenable Security Center User Guide*.

PHP Version

Upgraded to PHP 7.3.9.

Bug Fixes

Bug Fix	Defect ID
Resolved an issue viewing asset intersections on a repository.	00821563
Improved the error messaging around uploading zipped Nessus files.	00832235
Resolved an issue where previously mitigated vulnerabilities were being duplicated upon rediscovery.	00821464
Resolved an issue with editing usernames as an admin.	00810100
Updated Apache configs to prevent running in HTTP mode.	00781702
Resolved an issue with malformed characters in the Recast Risk database.	00778720
Resolved an issue with reports when no display columns were selected.	00640428
Resolved an issue where Apple devices would show up as a device on reports.	00557162

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and MD5 Checksums

Filenames and MD5 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.12.0:

Product	Tested Version
Nessus	8.5.1 and later
Log Correlation Engine	5.1.1 and later
Nessus Network Monitor	5.9.0 and later
Industrial Security	1.4.0 and later

Tenable Security Center 5.13.0 Release Notes (2019-12-30)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: Tenable recommends upgrading to the patch for this release, Tenable Security Center Patch 202102.1Tenable Security Center Patch 202103.1, which includes a fix for a potential vulnerability. For more information, see the Tenable Product Security Advisory.

If you are running version 5.6.2.1 or later, you can upgrade directly to version 5.13.0. If you are running a version earlier than 5.6.2.1, upgrade to version 5.6.2.1 before upgrading to version 5.13.0.

Tenable recommends performing a backup before upgrading Tenable Security Center. For more information, see Perform a Backup in the *Tenable Security Center User Guide*.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2.1 to 5.13.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

This release addresses multiple third-party vulnerabilities. For more information, see the Security Advisory.

You can download the update files from the Tenable Security Center Downloads page.

New Features

Lumin Synchronization

You can now send Tenable Security Center data to Tenable Lumin for analysis and reporting. Tenable Lumin is a cloud product (additional purchase required) that can quickly and accurately assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers in your Salesforce industry and the larger population.

Note: When data is sent from Tenable Security Center to Tenable Lumin, it may take 24 to 48 hours for the data to be completely processed.

For more information, see Lumin Synchronization in the *Tenable Security Center User Guide*.

API Key Authentication

Admin users can now authorize individual users to access Tenable Security Center through individual API keys as an authentication method.

For more information, see API Key Authentication in the *Tenable Security Center User Guide*.

SSL Certificate Passphrase Protection

You can now add passphrase protection when using SSL certificates to connect with Nessus, Tenable Network Monitor, or Industrial Security scanners.

For more information, see Nessus Scanners, Tenable Network Monitor Instance Settings, or Industrial Security Instance Settings in the *Tenable Security Center User Guide*.

Deprecated Features

With this release, Tenable Security Center has upgraded OpenSSL to 1.1.1. Once upgraded, FIPS compliance is no longer supported in Tenable Security Center.

Included Package Upgrades

- Apache 2.4.41
- SimpleSAML 1.17.7
- OpenSSL 1.1.1d
- OpenLDAP 2.4.48

Bug Fixes

Bug Fix	Defect ID
Resolved an issue where scans hung when run with IP Randomization enabled.	00901086, 00899516, 00910662, 00893442, 00838099
Resolved an issue where the administrator's license dashboard component did not properly display the expiration date for licenses that do not expire.	00893436
Resolved an issue where reports generated SIGSEGV errors following Tenable Security Center 5.12.0.	00902883, 00894719
Resolved an issue where scan chunks would be lost if the scanner	00882613

they were on crashed or was otherwise unreachable during the scan.	
Resolved issue where attempting to use empty data from session file in cases where action is not needed caused a PHP warning.	00888358
Resolved issue where session without stored username caused a PHP warning from a debug statement.	00888350
Resolved and issue where LCE clients could not be accessed in Tenable Security Center.	00870827
Prevented multiples of the same username on a Tenable Security Center instance.	00869817
Resolved an issue where error messages were not being properly displayed when uploading custom plugins.	00834254
Resolved an issue where long DNS search filters were not bounded by the text box.	00848504
Resolved an issue rendering large numbers on ARCs.	00844447
Resolved an issue where IPv6 proxies in Tenable Security Center would not resolve properly for downloading feed updates.	00818798
Allowed users to delete all dashboards.	00764302
Fixed an issue where the error handling for scanning would crash in certain circumstances.	00725607
Resolved an issue where users responsible for an asset were not properly disassociated from it when the asset was deleted.	00694951
Resolved an issue where the system information tab was not displaying OS information correctly.	00712966
Resolved errors with ASR Reports.	00711338
Resolved an issue with the Dashboard Viewport size.	00710336
Resolved issues with displaying notifications.	00675679

Prevented endless querying in System Logs.	00609692
Resolved issue saving the Vulnerability Mitigated filter.	00598571

API Changelog

For more information about the API changes for this release, see the Tenable Security Center API Changelog.

Filenames and MD5 Checksums

Filenames and MD5 checksums are located on the Tenable Security Center Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with Tenable Security Center 5.13.0:

Product	Tested Version
Nessus	8.5.1 and later
Log Correlation Engine	5.1.1 and later
Nessus Network Monitor	5.9.0 and later
Industrial Security	1.4.0 and later
OT Security	3.4.9 and later

Tenable Security Center 5.9.0 Release Notes (2019-02-11)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

If you are running version 5.5.0 or later, you can upgrade directly to version 5.9.0. If you are running a version earlier than 5.5.0, upgrade to version 5.5.0 before upgrading to version 5.9.0.

You can download the update files from the Tenable Downloads page.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2 to 5.9.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

New Features and Functionality

SAML / Shibboleth Integration

This integration adds support for Security Assertion Markup Language (SAML) 2.0 and Shibboleth 1.3, giving customers multiple SSO/authentication options to streamline their security with one-click log in, centralized authentication, and increased security and convenience.

Tenable Security Center now includes SimpleSAMLPHP 1.16.3 as a dependency when installing or updating Tenable Security Center.

For more information, see SAML Authentication in the *Tenable Security Center User Guide*.

Predictive Prioritization

A groundbreaking new innovation to help you understand the actual impact of the vulnerabilities in your environment so you can reprioritize vulnerabilities based on the probability that it will be leveraged in an attack. You will now see a new Vulnerability Priority Rating (VPR) for each vulnerability. This rating augments CVSS scores and represents the likelihood a given vulnerability will be exploited in the next 28 days, along with its severity. The rating is calculated nightly for every vulnerability Tenable tracks and factors in current threat intelligence information to help you prioritize vulnerabilities with the highest likelihood of impact to your organization. For more information view the Predictive Prioritization website.

For more information, see Vulnerability Analysis Filters in the *Tenable Security Center User Guide*.

Industrial Security Integration

This integration will allow Tenable Security Center customers with Industrial Security instances to import IS data into Tenable Security Center. This will give customers the ability to access Tenable Security Center's powerful reporting and dashboard features.

For more information, see Industrial Security Instances in the *Tenable Security Center User Guide*.

Automatic Scan Zone Distribution Restrictions

This new toggle will allow organizations with overlapping IP addresses in a scan zone to force a scanner to honor the restrictions based on the scan zones selected for a particular organization.

For more information, see Organizations in the *Tenable Security Center User Guide*.

Changed Functionality

- You can now filter by a combination of assets for agent data.
- Plugin 112154 no longer counts against a Tenable Security Center license.

Bug Fixes

- Resolved an issue where a caching issue caused invalid trend lines.
- Resolved an issue where combination assets did not work as expected.
- Resolved an issue in viewing and using LDAP and DNS assets.
- Resolved an issue submitting email addresses (user, reports, etc) that included special characters.
- Restored an API Field (“orgName” in /currentUser::GET) to resolve issues with customer scripts and integrations.
- Removed Scan Result ID from appearing in charts and report headings.
- Resolved an issue where some scanners generated excessive error messages to the System Log.
- Resolved an issue where scans would fail due to database errors.
- Resolved an issue when filtering by CVSS v2 or v3 scores in combination with other filters.
- Resolved an issue where credentials with privilege escalation did not work as expected.
- Resolved an issue where drilldowns into Scan Results would generate an error if the scan referenced Audit Files with some unexpected formatting issues.
- Resolved an issue where certificate-authenticated user accounts could not be edited to use another authentication method.
- Resolved an issue where filtering on the Report Results page using the finish time filter parameter "all" did not work as expected.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with SecurityCenter 5.9.0:

Product	Tested Version

Nessus	7.1.4 and later
Nessus Manager	7.1.4 and later
Log Correlation Engine	5.0.6 and later
Nessus Network Monitor	5.1.1 and later
3D Tool	2.0 and later
Industrial Security	1.3.0 and later

2018 Tenable Security Center

2018 Tenable Security Center

SecurityCenter 5.7.0 Release Notes (2018-07-31)

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

If you are running version 5.5.0 or later, you can upgrade directly to version 5.7.0. If you are running a version earlier than 5.5.0, upgrade to version 5.5.0 before upgrading to version 5.7.0.

> **Note:** If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.6.2 to 5.7.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

You can download the update files from https://www.tenable.com/downloads/securitycenter-3d-tool-and-xtool.

LIST CVES WITHIN PRODUCT, WHEN AVAILABLEFor more information, see the Security Advisory.

New Features

- Mobile Agent Workforce improvements:
  - SecurityCenter can now recognize unique agents from the same IP address using agent IDs.
  - New agent repository type for agent scan data.
  - Updated vulnerability analysis tools to integrate agent IDs.
- CVSS v3 support.
- Added the None option to the vulnerability analysis Patch Published filter to identify vulnerabilities without a patch.
- Added more options to vulnerability analysis time filters (Patch Published, Plugin Modified, Plugin Published, Vulnerability Published, Vulnerability Discovered, Vulnerability Last Observed, and Vulnerability Mitigated).
- Redesigned the credentials module.
- Added support for Lieberman credentials.
- Added support for BeyondTrust credentials.
- Upgraded to PHP 7.1.1.5.
- Upgraded to jQuery 3.3.1.

Bug Fixes

- "Hide Disabled" button breaks plugin details in scan policy.
- Fixed errors with port 0 in assets.
- No Response from showvulns When Viewing Scan Data by DNS Name Summary or When Attempting to Run a Report on Individual Scan.
- Error when viewing scan results, sorted by DNS name.
- Plugin Published/Modified Filters Non-functional when Filtering for Plugins in Scan Policy.
- "See also" section missing from MDM plugins in SecurityCenter.
- Credentialed Scan Failure report errors out with "Error DetailsError getting DataSource #120846 for Report Source...".
- Scans not honoring "Scan Timeout Action" setting.
- Remote Repository Username and Password Problem.
- Certificate Login Issues after enabling password complexity in SC 5.5.
- Customer is unable to go back in and edit report. Receives Validation Failed error.
- HTML not Parsing correctly when searching syslog text.

Upgrade Notes

If you previously configured agent scans in SecurityCenter, you must perform post-upgrade configuration steps to reconfigure agent scanning. First, create an agent repository for your agent scan data. Then, update your agent scan configurations to import data to the agent repository. You cannot import agent scan data into non-agent repositories.

Scan jobs from before the upgrade continue to run until you update the scan configuration.

Filenames and MD5 Checksums

Note: This release updates the .rpm file name from **es** to **el** to accurately reflect support for the Enterprise Linux architecture.

File	Product	MD5
SecurityCenter-5.7.0-	SecurityCenter 5.0 or	04087b9ede28422e03ca36bdeeed45b0

File	Product	MD5
el6.x86_64.rpm	later on CentOS 6 SecurityCenter 5.0 or later on Red Hat Enterprise Linux 6.0 Tenable Appliance 4.x	
SecurityCenter-5.7.0-el7.x86_64.rpm	SecurityCenter 5.0 or later on CentOS 7 SecurityCenter 5.0 or later on Red Hat Enterprise Linux 7.0	d3241843c0072646cb6d9a30f17fcfb5

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with SecurityCenter 5.7.0.

Product	Tested Version
Nessus	6.3.0 and later
Nessus Manager	7.1.0 and later
Log Correlation Engine	5.0.6 and later
Nessus Network Monitor	5.1.1 and later
3D Tool	2.0 and later

SecurityCenter 5.7.1 Release Notes (2018-09-17)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

If you are running version 5.5.0 or later, you can upgrade directly to version 5.7.1. If you are running a version earlier than 5.5.0, upgrade to version 5.5.0 before upgrading to version 5.7.1.

Note: If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.6.2 to 5.7.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

You can download the update files from https://www.tenable.com/downloads/securitycenter-3d-tool-and-xtool.

LIST CVES WITHIN PRODUCT, WHEN AVAILABLEFor more information, see the Security Advisory.

New Features

- Upgraded OpenSSL to 1.0.2p
- Upgraded PHP to 7.1.21
- Added "System Name" for Lieberman credentials
- Added "Admin URL" for Mobile Iron MDM mobile repositories
- Added Remote Repo Sync & Offline Repo Support for agent repositories
- Added X-Content-Type-Options headers to static files

Bug Fixes

- Optimized trending chart generation logic
- Missing agent_flush_vulns
- Plugin Family Summary tool not showing results when viewing scan results
- Reports crash with Showvulns errors SC 5.7
- After Updating To 5.7.0 Jobd Stops Running After User Login
- Client is getting a showvulns error when trying to run Unsupported OS Report
- Dynamic Assets Non-Functional
- Report unable to process due to invalid query
- Filter: Days-to-Mitigate not working properly
- Output Asset filter returns "No Results" for asset list with assets and vulns
- Trending Dashboard Components Not Honoring Repository Filter

- SC 5.7 Upgrade converts LDAP users linked to certificates
- Manual Combination of Assets In Filters Does Not Work
- Unable to Unpin Shared Dashboard if Filtering Enabled
- Truncated text for Chinese language
- Scan crashed due to memory consumption (memory_limit in php.in)
- SC 5.6 Maximum login attempts permitting 2 extra attempts
- LDAP ID may not be specified for authType tns
- LDAP selecting user is not populating first and last name field
- More flexibility to set job concurrency (requires support engagement) with new defaults for fresh installs

Filenames and MD5 Checksums

File	Product	MD5
SecurityCenter-5.7.1-el6.x86_64.rpm	SecurityCenter 5.0 or later on CentOS 6 SecurityCenter 5.0 or later on Red Hat Enterprise Linux 6.0 Tenable Appliance 4.x	37390ba40d2ac1cdc0292bed81ef7b9a
SecurityCenter-5.7.1-el7.x86_64.rpm	SecurityCenter 5.0 or later on CentOS 7 SecurityCenter 5.0 or later on Red Hat Enterprise Linux 7.0	318e2e166370febf812baccb945c22a1

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with SecurityCenter 5.7.1.

Product	Tested Version
Nessus	6.3.0 and later
Nessus Manager	7.2.0 and later
Log Correlation Engine	5.0.6 and later
Nessus Network Monitor	5.1.1 and later
3D Tool	2.0 and later

Tenable Security Center (Formerly SecurityCenter) 5.8.0 Release Notes (2018-11-07)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

If you are running version 5.5.0 or later, you can upgrade directly to version 5.8.0. If you are running a version earlier than 5.5.0, upgrade to version 5.5.0 before upgrading to version 5.8.0.

Note: If your upgrade path skips versions of Tenable Security Center (e.g., upgrading from 5.6.2 to 5.8.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

You can download the update files from the Tenable Downloads page.

For more information, see the Security Advisory.

New Features

- Resolve DNS assets in parallel
- Accept/recast support for agent data
- Expire agent data on its own schedule
- Reassign objects for users deleted by admins
- Set a date threshold to import data for agent scans

- Added the scan id in the component titles of PDF reports
- Clarified agent behavior on ASR/ARF reports

Bug Fixes

- Improved agent repository snapshot cleanup
- Errors with the Vulnerability Last Observed filter and overlapping ip addresses
- Error editing Smart Card/CAC card users
- Enabled sorting on dashboard columns
- Problems with SCAP scanning on RHEL
- Fixed the Initiator filter on System Logs
- Improved logging to /var/log/messages
- Uncaught errors with Netflow dashboard
- Stopped writing random characters to audit checks

Filenames and MD5 Checksums

Filenames and MD5 checksums are located on the Tenable Downloads page.

Tenable Integrated Product Compatibility

The following table lists the Tenable product versions tested with SecurityCenter 5.8.0:

Product	Tested Version
Nessus	6.3.0 and later
Nessus Manager	7.2.0 and later
Log Correlation Engine	5.0.6 and later
Nessus Network Monitor	5.1.1 and later
3D Tool	2.0 and later

OpenSSL Patch Release Notes (2018-01-15)

Tenable has released a patch for SecurityCenter 5.4.x, 5.5.x, and 5.6.0.x to update OpenSSL to version 1.0.2n. SecurityCenter 5.6.1 already contains the OpenSSL 1.0.2n update.

For more information, see the Security Advisory.

Contents

- libcrypto.so.1.0.0
- libssl.so.1.0.0
- openssl

Steps to Apply

1. Download the appropriate patch to SC box. Files are named `SC-201801.1-5.x.tgz` and can be placed anywhere, though tmp is a good choice.
2. Untar the patch file: `tar zxf SC-201801.1-5.x.tgz`.
3. Change the directory to the extracted directory `cd SC-201711.1-5.x`.
4. Run the install: `sh ./install.sh`.

Third-Party Product Updates

Third-Party Product	Updated to Address
OpenSSL 1.0.2n-fips	CVE-2017-3737 CVE-2017-3738

File Names and MD5 Checksums

File	MD5
SC-201801.1.5.x-rh6-64.tgz	7148fec63713eb4ae882af85ec4c1fc6
SC-201801.1.5.x-rh7-64.tgz	e230e49e9dc9a6e2b1cacd432d9e1b4b

SecurityCenter 5.6.2 Release Notes (2018-03-19)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Upgrade Notes

> **Note:** If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.6.2), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

- If you are running version 4.8.2 or later, upgrade to version 5.4.0 before upgrading to version 5.6.2.
- If you are running version 5.4.0 or later, upgrade directly to 5.6.2.
- Added additional fields for Cyberark AIM Web Service credentials, including the ability to add certificate files
- Updated the embedded documentation (accessed from any page of the SecurityCenter interface using the **Username > Help** menu) to parallel the SecurityCenter User Guide: https://docs.tenable.com/security-center/Content/Welcome.htm.

Bug Fixes

- Exploitable by Malware dashboard displays some vulnerability names as 'N/A'
- Error codes should be parsed as integers before processing
- Adding key without comment breaks ability to use feature
- Feed notice seen in logs
- SC 5.6.1 MySQL Credential Validation Failed - Map not found for dbType 'MySQL'.
- Sudo SSH credentials from SecurityCenter with sudo path not working the same way as scans from Nessus
- Credentialed Scan Failure report errors out with "Error DetailsError getting DataSource #120846 for Report Source..."
- SC not accepting hostname in hostname field for LDAP
- Windows software inventory report formatting
- Ticket Assignee summary components only show tickets for the currently logged in user
- Monthly Scan Schedule: Issues with selecting "day of the week"
- Bad feed updates should not crash a SecurityCenter instance

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.6.2-es6.x86_64.rpm	50713fda35380ce75049e62ea7c81aec
SecurityCenter-5.6.2-es7.x86_64.rpm	c257b00c3ee301a50c92d562b00717b4

Showvulns Patch Release Notes (2018-03-23)

Apply this patch to SecurityCenter installations running version 5.6.2. The fixes in this patch resolve several issues related to a showvulns bug.

> **Note:** You do not need to apply this patch to SecurityCenter installations running earlier versions.

Contents

- showvulns
- showvulns-archive
- showvulns-individual

Fixed an issue where Exploit Available always displayed "False" on the Vulnerability Detail View page.

Resolved errors that occur when evaluating queries using the Vulnerability Details tool.

Steps to apply

> **Note:** If you are applying the patch to a Tenable Appliance, you must enable SSH access as described in the Tenable Appliance User Guide. If you are running a Tenable Appliance version earlier than 4.4.0, contact Support for assistance.

1. Download the appropriate patch to SecurityCenter. The files are named `SC-201803.1-5.6.2-rh6-64.tgz` and `SC-201803.1-5.6.2-rh7-64.tgz` and can be placed anywhere, though `/tmp` is a good choice.
2. Untar the patch file: `tar zxf SC-201803.1-5.6.2-rh6-64.tgz`
3. Change the directory to the extracted directory: `cd SC-201803.1-5.6.2-rh6-64`
4. Run the install: `sh ./install.sh`

File Names & MD5 Checksums

File	MD5
SC-201803.1-5.6.2-rh6-64.tgz	dd5c6e096e9354ece0c4a1ae32e22b5a
SC-201803.1-5.6.2-rh7-64.tgz	cbf51e6cac45f0316c74345a3764d1c8

SecurityCenter 5.6.2.1 Release Notes (2018-04-05)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Upgrade Notes

- This release integrates the Showvulns Patch completed to fix various issues from SecurityCenter version 5.6.2.
- If you are running version 4.8.2 or later, upgrade to version 5.4.0 before upgrading to version 5.6.2.1.
- If you are running version 5.4.0 or later, upgrade directly to 5.6.2.1.

Note: If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.6.2.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes

- Fixed an issue where Exploit Available always displayed "False" on the Vulnerability Detail View page.
- Resolved errors that occur when evaluating queries using the Vulnerability Details tool.
- Upgraded PHP to version 5.6.34
- Improved performance for installs with a large number of scan results.

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.6.2.1-es6.x86_64.rpm	63c748f5049d5d5ac5367ef9f4487197
SecurityCenter-5.6.2.1-es7.x86_64.rpm	beb997711d10f8c20e6c9864384c1e12

PHP Patch Release Notes (2018-04-26)

Apply this patch to SecurityCenter installations running version 5.0 to 5.6.x. This patch updates PHP to version 5.6.34 to address CVE-2018-7584.

For more information, see the Security Advisory.

Caution: Do not apply this patch to SecurityCenter installations running version 5.7.0 or later.

Contents

- libphp5.so
- php

Steps to Apply

Note: If you are applying the patch to a Tenable appliance, you must enable SSH access as described in the Tenable Appliance User Guide. If you are running a Tenable Appliance version earlier than 4.4.0, contact Support for assistance.

1. Download the appropriate patch to SecurityCenter or your appliance. The files can be placed anywhere, though /tmp is a good choice.

2. Untar the patch file: `tar zxf SC-201804.1-5.x.tgz`

3. Change the directory to the extracted directory: "cd SC-201804.1-5.x"

4. Run the install: "sh ./install.sh"

File Names & MD5 Checksums

File	Product	MD5
SC-201804.1.5.x-rh6-64.tgz	SecurityCenter 5.0 or later on CentOS 6 Tenable appliance 4.x	b8682a1cc83e27310ec137624e963bb6
SC-201804.1.5.x-rh7-64.tgz	SecurityCenter 5.0 or later on CentOS 7	bc94eae31d28191d8e1b734bc91acb3e

SecurityCenter OpenSSL 1.0.2o Patch Release Notes (2018-05-08)

Apply this patch to SecurityCenter installations running version 5.0 or later. This patch updates OpenSSL to version 1.0.2o-fips to address CVE-2017-3738, CVE-2018-0733, and CVE-2018-0739.

For more information, see the Security Advisory.

Contents

- libcrypto.so.1.0.0
- libssl.so.1.0.0
- openssl

Steps to Apply

Apply the patch to your SecurityCenter or Tenable Appliance deployment.

Apply the patch to a standalone Tenable Security Center:

> **Note:** SecurityCenter automatically restarts during installation.

1. Download the patch to SecurityCenter. You can save the files in any location (e.g., `/tmp`).
2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation begins and SecurityCenter is stopped. After the installation finishes, SecurityCenter automatically restarts.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.
2. Download the patch to your Appliance. You can save the files in any location (e.g., `/tmp`).
3. Stop the SecurityCenter instance from Appliance, as described in Manage SecurityCenter.
4. Run the following command to untar the patch file:

   ```
   tar zxf filename.tgz
   ```

5. Run the following command to change the directory to the extracted directory:

   ```
   cd directory
   ```

6. Run the following command to begin the installation:;

   ```
   sh ./install.sh
   ```

   The installation runs and finishes.

7. Start SecurityCenter from Appliance, as described in Manage SecurityCenter.

Filenames and MD5 Checksums

File	Product	MD5
SC-201805.1-5.x-rh6-64.tgz	SecurityCenter 5.0 or later on CentOS 6 Tenable appliance 4.x	60b2a98ef073a819fd33f636d786d404
SC-201805.1-5.x-rh7-64.tgz	SecurityCenter 5.0 or later on CentOS 7	214c02c19c61f3166159dc0061c7be7f

SecurityCenter 5.7.0 Patch Release Notes (2018-08-14)

Apply this patch to SecurityCenter installations running version 5.7.0 or later. This corrects issues arising from filtering on multiple assets on Vulnerability Analysis pages.

Contents

- install.sh
- VulnLib.php

Steps to Apply

Apply the patch to a standalone Tenable Security Center:

1. Download the patch from https://www.tenable.com/downloads/securitycenter-3d-tool-and-xtool to SecurityCenter. You can save the files in any location (e.g., /tmp).
2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf SC-201808.1-5.7.0.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   cd directory

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.
2. Download the patch from https://www.tenable.com/downloads/securitycenter-3d-tool-and-xtool to your Appliance. You can save the files in any location (e.g., /tmp).
3. Run the following command to untar the patch file:

   ```
   tar zxf SC-201808.1-5.7.0.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   cd directory

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs.

Filenames and MD5 Checksums

File	Product	MD5
SC-201808.1-5.7.0.tgz	SecurityCenter 5.0 or later on CentOS 6 or 7 SecurityCenter 5.0 or later on Red Hat Enterprise Linux 6.0 Tenable Appliance 4.x	9791fdedda7c8de25b538dd113690a7f

Tenable Security Center 201811.1 Patch Release Notes (2018-11-13)

Apply this patch to SecurityCenter installations running version 5.7.1 and earlier. This patch updates Apache Xalan and Serializer to version 2.7.2 to address:

- CVE-2013-2153
- CVE-2013-2154
- CVE-2013-2155
- CVE-2013-2156
- CVE-2013-2210
- CVE-2013-4517
- CVE-2014-0107

Contents

- serializer-2.7.2.jar
- xalan-2.7.2.jar

Steps to Apply

Apply the patch to a standalone Tenable Security Center:

1. Download the patch from the Tenable Downloads page to SecurityCenter. You can save the files in any location (e.g., /tmp).

2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf SC-201811.1-5.x.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd SC-201811.1-5.x
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.

2. Download the patch from the Tenable Downloads page to your Appliance. You can save the files in any location (e.g., /tmp).

3. Run the following command to untar the patch file:

   ```
   tar zxf SC-201811.1-5.x.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd SC-201811.1-5.x
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes.

Filenames and MD5 Checksums

Filenames and MD5 checksums are located on the Tenable Downloads page.

Tenable Security Center Patch 201812.1-5.8.0 Release Notes (2018-12-03)

Apply this patch toTenable Security Center installations running version 5.8.0. This patch fixes updating DNS and LDAP Asset Lists.

Contents

- CachedHostnameResolver.php
- ResolveHostnamesBase.php

Steps to Apply

Apply the patch to a standalone Tenable Security Center:

1. Download the patch from The Tenable Downloads Page. You can save the files in any location (e.g., /tmp).
2. Access the command line as a user with root-level permissions.

   > **Note:** If your organization does not have root-level users, contact Tenable Support for assistance.

3. Run the following command to untar the patch file:

   ```
   tar zxf SC-201812.1-5.8.0.tgz
   ```

4. Run the following command to change the directory to the extracted directory:

   ```
   cd SC-201812.1-5.8.0
   ```

5. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs.

Apply the patch to a Tenable Appliance:

1. Enable SSH access, as described in SSH User Access. If you are running a Tenable Appliance version earlier than 4.4.0, contact Tenable Support for assistance.
2. Download the patch from https://www.tenable.com/downloads/securitycenter-3d-tool-and-xtool to your Appliance. You can save the files in any location (e.g., /tmp).
3. Stop the SecurityCenter instance from Appliance, as described in Manage SecurityCenter.
4. Run the following command to untar the patch file:

   ```
   tar zxf SC-201812.1-5.8.0.tgz
   ```

5. Run the following command to change the directory to the extracted directory:

   ```
   cd SC-201812.1-5.8.0
   ```

6. Run the following command to begin the installation:

   ```
   sh ./install.sh
   ```

   The installation runs and finishes.

Filenames and MD5 Checksums

File	Product	MD5
SC-201812.1-5.8.0.tgz	SecurityCenter 5.8.0 or later on CentOS 6 or CentOS 7 SecurityCenter 5.8.0 or later on Red Hat Enterprise Linux 6.0 or Red Hat Enterprise Linux 7.0 Tenable Appliance 4.x	d5fec7619d4e638fb290c88f70b6fcb2

2017 Tenable Security Center

2017 Tenable Security Center

SecurityCenter 5.4.3 Release Notes - 2/9/2017

Apache Patch Release Notes - 2/17/2016

File Upload Patch Release Notes - 2/17/2016

PHP and OpenSSL Patch Release Notes - 2/17/2016

SecurityCenter 5.4.4 Release Notes - 3/1/2017

SecurityCenter 5.4.5 Release Notes - 3/21/2017

SecurityCenter 5.5.0 Release Notes - 6/6/2017

SecurityCenter 5.5.1 Release Notes - 7/25/2017

PHP Patch Release Notes - 9/8/2017

SecurityCenter 5.5.2 Release Notes - 10/2/2017

PHP Patch Release Notes - 11/2/2017

SecurityCenter 5.6.0 Release Notes (2017-11-02)

SecurityCenter 5.6.0.1 Release Notes (2017-11-10)

PHP Release Notes (2017-11-17)

SecurityCenter 5.6.1 Release Notes (2017-12-18)

2017 Tenable Security Center

SecurityCenter 5.4.3 Release Notes - 2/9/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.4.3, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.4.3 includes the following capability improvement:

- **Additional SSO Support** - SecurityCenter has added support for IBM Security Access Manager

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.4.3 supports the following direct upgrade paths:

- 4.8.2 > 5.4.3
- 5.[0-3] > 5.4.3

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.4.3. For more information about upgrading to SecurityCenter 5.4.3, refer to the SecurityCenter 5.4 User Guide.

If you are using Nessus agents, SecurityCenter 5.4.3 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

> **Note**: Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.4.3-es5.x86_64.rpm	d7fdadb667479db2f2ca4e62969a3b56

File	MD5
SecurityCenter-5.4.3-es6.x86_64.rpm	4a15e86cefb0a41c42813518225c0ea2
SecurityCenter-5.4.3-es7.x86_64.rpm	3169c2cef5473fd7eb6e6d1ff4e395fe

Resolved Items

Summary	Issue Number
Clean up scan result behavior	296496
Plugin Family column not included in CSV report	352896
IP Summary does not display repository column	341216
Plugins being disabled on policy creation	334908
Send scan result to report does not properly encode matrices	329475
Renaming a credential resets the escalation password	319133
Only allow appropriate repository when focusing report queries	309881
Largest ipCount not displaying on Asset List	304889
Submitting an existing policy before it fully loads disables all plugins	358752
Toggling from mitigated to cumulative does not update the "Last Observed" column	305455
Mitigated filters should be passed to Export CSV calls	323533
Slow filtering for large number of assets	296020

Apache Patch Release Notes - 2/17/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 5.0.2, 5.1.0, 5.2.0, 5.3.1, 5.3.2, 5.4.0, and 5.4.2 that updates Apache to 2.2.32.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201702.1-5.x-rh5-64.tgz	293d373e771ec53b9da6e25eaf7c8649
SC-201702.1-5.x-rh6-64.tgz	4f63a6cad169fb4d1f050482754f8b70
SC-201702.1-5.x-rh7-64.tgz	4e88259f1220a422614ac1dd662ba945

File Upload Patch Release Notes - 2/17/2016

Tenable has released a patch script for SecurityCenter 5.4.0, 5.4.2, and 5.4.3 that prevents file removal with a specially crafted file upload.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Name & MD5 Checksum

File	MD5
SC-201702.2-5.4.x.tgz	ccb023d32e1a99e2c11277cf8e606c64

PHP and OpenSSL Patch Release Notes - 2/17/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 5.0.2, 5.1.0, 5.2.0, 5.3.1, 5.3.2, 5.4.0, and 5.4.2 that updates PHP to 7.1.2 and addresses the OpenSSL vulnerabilities. This version bundles an updated OpenSSL library version (1.1.0e) that is not affected.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201702.3-5.x-rh5-64.tgz	6024d46d82839aa95763fc28b3a48d60
SC-201702.3-5.x-rh6-64.tgz	bfc2808658fa555de3f7e6af5c0d0d8c
SC-201702.3-5.x-rh7-64.tgz	335964c9e7436f4477277509a033e1dd

SecurityCenter 5.4.4 Release Notes - 3/1/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.4.4, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.4.4 includes the following capability improvements:

- A fix to a vulnerability detected in PHP code
- Other minor bug fixes

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.4.4 supports the following direct upgrade paths:

- 4.8.2 > 5.4.4
- 5.[0-3] > 5.4.4

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.4.4. For more information about upgrading to SecurityCenter 5.4.4, refer to the SecurityCenter 5.4 User Guide.

If you are using Nessus agents, SecurityCenter 5.4.4 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.4.4-es5.x86_64.rpm	ac77ee89a34078cb22b99ffd2e71b88d
SecurityCenter-5.4.4-es6.x86_64.rpm	84e652adcff3c8cfb17a12f70aec3fe5
SecurityCenter-5.4.4-es7.x86_64.rpm	757b993840bc146320544dd44bd41845

Resolved Items

Summary	Issue Number
Group Summary behavior bug	304412
Unserialize exploit in PHP	370733
DB Object call bug	304412

SecurityCenter 5.4.5 Release Notes - 3/21/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.4.5, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.4.5 includes the following capability improvement:

- A fix to a bug that caused upgrades to fail in certain limited cases

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.4.5 supports the following direct upgrade paths:

- 4.8.2 > 5.4.5
- 5.[0-3] > 5.4.5

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.4.5. For more information about upgrading to SecurityCenter 5.4.5, refer to the SecurityCenter 5.4 User Guide.

If you are using Nessus agents, SecurityCenter 5.4.5 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.4.5-es5.x86_64.rpm	16ed6558383108f17ae9688b0eca81fb
SecurityCenter-5.4.5-es6.x86_64.rpm	533cb652772fc542997916ebb27dd042
SecurityCenter-5.4.5-es7.x86_64.rpm	ccb0738cca9d698ecfc9ae818229a6f0

SecurityCenter 5.5.0 Release Notes - 6/6/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.5.0, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.5.0 includes the following capability improvements:

- **Thycotic Secret Server Support -** Customers can now utilize Thycotic to manage credentials used for scanning
- **Improved password control -** Customers can now control password expiration and complexity in SecurityCenter
- **Support for translated plug-ins -** Customers can now select plug-in languages in SecurityCenter, including plug-ins translated into Japanese, Chinese (Simplified), and Chinese (Traditional)

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.5.0 supports the following upgrade paths:

- If you are running version 4.8.2 or later, upgrade to version 5.4.0 before upgrading to version 5.5.0.
- If you are running version 5.4.0 or later, upgrade directly to version 5.5.0.

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.5.0. For more information about upgrading to SecurityCenter 5.5.0, refer to the SecurityCenter 5.5 User Guide.

> **Note:** If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.5.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

If you are using Nessus agents, SecurityCenter 5.5.0 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

> **Note**: Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.5.0-es5.x86_64.rpm	36166a541a26b490262bfc309688ff46
SecurityCenter-5.5.0-es6.x86_64.rpm	7be951542451c5d6c8acb075acf9b694
SecurityCenter-5.5.0-es7.x86_64.rpm	e66a1e566e05f7a1774b768cd889c512

Resolved Items

Summary	Issue Number
SQL Error stopping SecurityCenter service	367862
Get trending working with data	374651
Directory traversal possible (DashboardLib.php)	377839
LCEStatus.php imports vulns every 15m regardless of "PassiveScannerResultsInterval"	375515
Endpoint /analysis::POST fails to sort on field DNS name for tool "sumip"	374932
Flush log writes sooner than currently in Jobd.php	367862
Migration to 5.5+ incorrectly displays "failed to restore" message	377905

Summary	Issue Number
Clean up group permissions on user add/edit	341459
Double calls made when editing a dashboard component	304412
Scan Copied Deletion and Edit - Does not delete Schedule	264241
Incorrect column list is displayed for CSV export of VDL	262690

SecurityCenter 5.5.1 Release Notes - 7/25/2017

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.5.1, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.5.1 includes the following capability improvements:

This point release of SecurityCenter fixes several recently discovered bugs related to Security Content Automation Protocol (SCAP) scans. Previously, when a user attempted to upload a Scap-Oval audit file to SecurityCenter, the application would not display benchmarks and a validation error, "Invalid AuditFile" would be displayed to the user. Now, a SCAP-OVAL audit file can be uploaded (and submitted) with Benchmark Type OVAL Unix or OVAL Windows (by both admin user and org user). Once an SCAP-OVAL audit file is uploaded, it can be viewed, edited, shared, and deleted.

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation

Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.5.1 supports the following upgrade paths:

- If you are running version 4.8.2 or later, upgrade to version 5.4.0 before upgrading to version 5.5.1.
- If you are running version 5.4.0 or later, upgrade directly to version 5.5.1.

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.5.1. For more information about upgrading to SecurityCenter 5.5.1, refer to the SecurityCenter 5.5 User Guide.

> **Note:** If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.5.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

If you are using Nessus agents, SecurityCenter 5.5.0 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

> **Note**: Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.5.1-es6.x86_64.rpm	b1c790ebe1ff7c7ca738b120a6b4fd2a
SecurityCenter-5.5.1-es7.x86_64.rpm	760401bc0168b06c3936e2aaaf76401e

PHP Patch Release Notes - 9/8/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 5.3.2, 5.4.0, 5.4.2, 5.4.5, 5.5.0, 5.5.1 and 5.5.2 that updates PHP to 5.6.31.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201708.1-5.x-rh5-64.tgz	13b7633389a80fb04da4fc918a8abda8
SC-201708.1-5.x-rh6-64.tgz	0264e2e9c8631e51261fc4a4e9be734f
SC-201708.1-5.x-rh7-64.tgz	e4ca7cdb4ce7bca0a11b5bdcd3fdf4e6

SecurityCenter 5.5.2 Release Notes - 10/2/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This release of SecurityCenter adds support for multiple LDAP servers. Users can now use multiple LDAP servers to authenticate SecurityCenter users. A PDF file of these release notes is also available here.

SecurityCenter 5.5.2 updates PHP to 7.1.7, for more information, see PHP Patch Release Notes.

New Features and Enhancements

Multi-LDAP support

This release adds support for use of multiple LDAP servers in SecurityCenter (moved from the Configuration page to Resources > LDAP Servers). This allows users to provide access to SecurityCenter using multiple LDAP servers, and allows compliance with local security policies..

Users can also now set up multiple LDAP Query assets for use in scanning, dashboards, and reports. For more information, see the official documentation at docs.tenable.com.

Limitations

- No support for duplicate names on a single LDAP Server: An LDAP Server could contain duplicate usernames. Currently, you cannot set up two SecurityCenter users who have the same LDAP names.
- Customers will not be able to set up org and admin user roles that share a single LDAP user: Customers will need to create two LDAP users–one for an admin, and one for an org if they want one user to have access to two roles.

Bug Fixes

- Fixed an issue with Agent Sync jobs in debug mode
- Fixed an issue where the delete option would not display on View Scan Result page for Scan Result with "Error" status
- Fixed an issue where the search field displays 'Search Undefined' instead of the content type of what is being searched when user is on any of the "Add Screens" (dashboard, report, component, ARC, or asset)
- Fixed an issue where the times listed in SC Setup file of the diagnostics archive are improperly formatted
- Fixed an issue where previewing an agent scanner with no results produces errors in the SC error log
- Fixed an issue where the word total was getting cut off when a user was adding a table component
- Fixed an issue where scans were being displayed as enabled when initially copied between groups
- Fixed an issue with the "Enable Cached Fetching" setting when creating a user. Once you clicked into the policy to utilize the feature, you'd see that at the bottom of the policy on the plugins tab it would say “Caching disabled for current user. Enable Caching” even if enabled.
- Fixed an issue where user was unable to upload Agent Scans when the Manager uses certificate authentication

- Replaced SHA1 library to support IE11
- Fixed login page so that username field is focused on load

Migration Notes

If an LDAP server was properly configured before migration, an LDAP Server will be created during migration. We strongly recommend that you copy all existing LDAP settings before migration. All organizations on the SC installation will be given access to this LDAP. Users can choose to go in and revoke access afterwards.

Other than that, no additional work is required to migrate existing LDAP setups in SecurityCenter.

Users can upgrade directly from 5.4.x or later to 5.5.2.

Users running versions of SecurityCenter earlier than 5.4.x need to first upgrade to 5.4.x, and then to 5.5.2.

> **Note:** If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.5.2), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.5.2-es6.x86_64.rpm	66d050c9eab7be1d2493def926268d80
SecurityCenter-5.5.2-es7.x86_64.rpm	717efdf5985a4702be40271681f4374e

PHP Patch Release Notes - 11/2/2017

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a PHP file update to SecurityCenter 5.5.0, 5.5.1 and 5.5.2 that prevents diagnostic scan password from allowing statements to be run against SC SQLite databases.

For more information, see the Security Advisory.

Steps to Apply:

1. Download appropriate patch to SC box. Files are named SC-201710.1-5.5.x.tgz and can be placed anywhere, though tmp is a good choice.
2. Untar patchfile tar zxf SC-201710.1-5.5.x.tgz
3. Change directory to the extracted directory cd SC-201710.1-5.5.x
4. Stop SecurityCenter: service SecurityCenter stop
5. Verify all jobs have finished: ps aux | grep tns
6. Run the install.sh ./install.sh
7. Start SecurityCenter: service SecurityCenter start

File Names & MD5 Checksums

File	MD5
SC-201710.1-5.5.x.tgz	21b0b57d08ebd39e1a3db8f9195417d8

SecurityCenter 5.6.0 Release Notes (2017-11-02)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Caution: SecurityCenter 5.6.0 was removed and replaced with SecurityCenter 5.6.0.1. For more information about the critical fixes in SecurityCenter 5.6.0.1, see the SecurityCenter 5.6.0.1 Release Notes (2017-11-10).

New Features and Enhancements

- Pendo data acquisition – Customers can now enable Pendo data acquisition to anonymously help Tenable prioritize feature enhancements and improve user experience in future releases. Enabling Pendo allows Tenable to collect anonymous usage statistics about customers' SecurityCenter deployments. No customer identifying information will be collected. This usage information will help guide our roadmap and prioritize enhancements for the most frequently used features. The Pendo feature will be disabled by default and can be enabled in the SecurityCenter privacy settings.

- Multi-Threaded C – Customers will now have performance and speed increases made possible with multi threading. This includes:
    - Up to a 50% reduction in time for dynamic asset preparation for larger data sets
    - Increased speed for Plugin Text searches and for complex searches on Plugin Output
    - Increased speed for Recast/Accept
- Plugin Filtering – Customers now have the ability to filter plugins by family type, such as Backdoors or Brute Force attacks. This advanced scanning capability saves time and increases productivity by providing a comprehensive view of each plugin associated with a specific family type.

Upgrade Notes:

- If you are running version 4.8.2 or later, upgrade to version 5.4.0 before upgrading to version 5.6.0.1.
- If you are running version 5.4.0 or later, upgrade directly to version 5.6.0.1.

> **Note:** If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.6.0), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes

- Plugin policy SQL injection + unsupported operands, etc.
- Missing Search String When Creating User
- Diagnostic scan password allows statements to be run against SC SQLite databases
- SC Error when modifying dashboard components with absolute date range
- New repository generates showvulns error - vulnerability analysis impacted
- Accept Risk rule removes some plugins from the Repo

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.6.0-dev-es6.x86_64.rpm	be3f89c66884e4c272ebab478d9b97a6

File	MD5
SecurityCenter-5.6.0-dev-es7.x86_64.rpm	8359442ee69f471e5e83058caae4559b

SecurityCenter 5.6.0.1 Release Notes (2017-11-10)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released SecurityCenter 5.6.0.1, a replacement for SecurityCenter 5.6.0. This resolves a critical issue with scan data imports being stuck in a pending state.

Upgrade Notes:

- If you are running version 4.8.2 or later, upgrade to version 5.4.0 before upgrading to version 5.6.0.1.
- If you are running version 5.4.0 or later, upgrade directly to version 5.6.0.1.

Note: If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.6.0.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Third-Party Product Updates

SecurityCenter 5.6.0.1 also includes the following third-party updates.

Third-Party Product	Updated to Address
PHP version 5.6.32	CVE-2016-1283
Open SSL 1.0.2m-fips	CVE-2017-2735 CVE-2017-3736

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.6.0.1-es6.x86_64.rpm	20619f98b9ee041ed74bcba995f3f020
SecurityCenter-5.6.0.1-es7.x86_64.rpm	f843dd96692158ccb8b406e81bd519cb

PHP Release Notes (2017-11-17)

This patch will update php to 5.6.32, and open SSL to 1.0.2m for SecurityCenter versions 5.4.0 and greater. Note that SecurityCenter 5.6.0.1 already has the upgrades in place.

For more information, see the Security Advisory.

Contents

- libcrypto.so.1.0.0
- libssl.so.1.0.0
- openssl
- libphp5.so
- php

Steps to Apply

1. Download appropriate patch to SC box. Files are named SC-201711.1-5.x.tgz and can be placed anywhere, though tmp is a good choice.

2. Untar patchfile tar zxf SC-201711.1-5.x.tgz

3. Change directory to the extracted directory cd SC-201711.1-5.x

4. Run the install: sh ./install.sh

Third-Party Product Updates

Third-Party Product	Updated to Address
PHP version 5.6.32	CVE-2016-1283
Open SSL 1.0.2m-fips	CVE-2017-3735 CVE-2017-3736

File Names & MD5 Checksums

File	MD5
SC-201711.1-5.x-rh6-64.tgz	ae9c026dafb0dee7ea3be1ae1a6d317e
SC-201711.1-5.x-rh7-64.tgz	4cdb06a5fcb8d8819a05e4bfbbd130f4

SecurityCenter 5.6.1 Release Notes (2017-12-18)

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Upgrade Notes

- Cyberark update: We have added additional fields for the Cyberark AIM Web Service
- If you are running version 4.8.2 or later, upgrade to version 5.4.0 before upgrading to version 5.6.1.
- If you are running version 5.4.0 or later, upgrade directly to version 5.6.1.

Note: If your upgrade path skips versions of SecurityCenter (e.g., upgrading from 5.4.0 to 5.6.1), Tenable recommends reviewing the release notes for all skipped versions. You may need to update your configurations because of features and functionality added in skipped versions.

Bug Fixes

- The column "vault_cyberark_url" column was missing from the "AppSSHCredential" and "SSHCredential" tables on a upgrade.
- SCAP Scan import fix
- Allow users to set the default timeframe for scan results
- Repository import fix between multiple SecurityCenter instances.
- Remote Repository Username / Password fix
- Renamed Enabled Cached Fetching field
- “CyberArk Account Details Name” is set to “true” for SSH CyberArk Vault credential with su privilege escalation
- Scans stuck during import fix
- Thycotic authentication fix
- IAVM 2017-A-0327 Multiple Vulnerabilities in OpenSSL fix upgraded version of OpenSSL to 1.0.2n
- Scans stuck in pending fix reenabled multithreading for scan imports

- Security Center 5.5.2 - LDAP fix allow SC users to associate with different LDAP servers after getting created.
- Customer can now create user/define a scan using install account when managed by SC
- SQL error: too many attached databases fix
- Fixed error while running query: URL: rest/lce/eventTypes?fields=df [GET] fixed error parsing utf-8 characters in custom LCE types

Third-Party Product Updates

For more information, see the Security Advisory.

Third-Party Product	Updated to Address
OpenSSL 1.0.2n-fips	CVE-2017-3737 CVE-2017-3738

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.6.1-es6.x86_64.rpm	4e80796c8acbb20b4213b9eb89332230
SecurityCenter-5.6.1-es7.x86_64.rpm	ea045e973d02906bda359e411b4c1d06

2016 Tenable Security Center

SecurityCenter 5.4.2 Release Notes - 12/7/2016

2016 Tenable Security Center

OpenSSL 1.0.1q Patch Release Notes - 1/6/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.6.2.2, 4.7.1, 4.8.2, 5.0.0.1, 5.0.2, and 5.1.0 that addresses the OpenSSL vulnerabilities. This version bundles an updated OpenSSL library version (1.0.1q) that is not affected.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201601.1-4.x-rh5-32.tgz	87723711f52f1c22279a1597c445e387
SC-201601.1-4.x-rh5-64.tgz	658fd17c6ee435f99612b72958da8170
SC-201601.1-4.x-rh6-32.tgz	ca9876612e3646d55ff455e3b614b08a
SC-201601.1-4.x-rh6-64.tgz	ff9027d2315bba4650d74d3a9d723765
SC-201601.1-5.x-rh5-64.tgz	4f7a4666232874226345589000c92edd
SC-201601.1-5.x-rh6-64.tgz	1ffc0779572997a753e575acc6d7772b

PHP Patch Release Notes - 3/8/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 5.0.2, 5.1.0, and 5.2.0 that updates PHP to 5.6.18.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201603.1-5.x-rh5-64.tgz	e4beebfb83b9b7928b6b61687d1129e4
SC-201603.1-5.x-rh6-64.tgz	eb983017056435d43d0ca4dc75b71010

SecurityCenter 5.3 Release Notes - 3/28/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.3, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.3 includes the following new notable capabilities:

- **Red Hat Enterprise Linux 7 and CentOS 7 support**: SecurityCenter 5.3 is now supported on the latest release of Red Hat Enterprise Linux 7 and CentOS 7.
- **Configurable user session limits**: SecurityCenter 5.3 now allows an administration to optionally set a max number of sessions per user for logon to the SecurityCenter UI.
- **User account logon notification**: SecurityCenter 5.3 administrators can display a user notification at logon time, which includes the time of the last successful logon, last failed logon attempt, and number of failed logons.

- **Scan status displays scanner distribution information**: SecurityCenter 5.3 now allows users to view detailed scan status information such as the scanners being utilized by the scan and the number of IP addresses distributed to each scanner.
- **Enhanced vulnerability mitigation logic**: SecurityCenter 5.3 improves validation of vulnerability resolution through intelligent authentication tracking.

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.3 supports the following direct upgrade paths:

- 4.8.1+ > 5.3
- 5.0+ > 5.3

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.1 prior to upgrading to SecurityCenter 5.3. For more information about upgrading to SecurityCenter 5.3, refer to the SecurityCenter User Guide.

If you are using Nessus agents, SecurityCenter 5.3 requires Nessus Cloud or Nessus Manager 6.5 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 4.0 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.2 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter 5 API, refer to the SecurityCenter 5 API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.3.0-es5.x86_64.rpm	fda9571114935f9e18f2a27128433719
SecurityCenter-5.3.0-es6.x86_64.rpm	92195775fbd8f2416c3c7c88af288a25
SecurityCenter-5.3.0-es7.x86_64.rpm	07b08ea4f781d0120af84c469cb10dea

Resolved Items

Below is a brief description of the most significant items resolved in the Security Center 5.3 release:

Summary	Issue Number
Export of Basic Network Scan policy disables all plugin families	00215150
Report Color Code Mismatch	00193717
Delete Recast/Accept Risk Rules	00168462
Nessus Agent Sync Timeouts not always set during upgrade	00193558
Create Monthly scan, Start time is not set correctly	00206452, 00176444
Agent results generate plugin names incorrectly	00198630
"Mitigated On" date is missing in PDF report	00194610, 00183942
Reports run with Now schedule should give indication they have launched	00150879
Admin account cannot lock/unlock initial security manager account	00185414
Filter in Report Results cannot be saved	00160589
Show IP Detail Error With Class A, Class B, Class C Summaries	00183611

SecurityCenter 5.3.1 Release Notes - 4/1/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.3.1, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click “Activation Codes”. Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.3.1 supports the following direct upgrade paths:

- 4.8.1+ > 5.3.1
- 5.0+ > 5.3.1

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.1 prior to upgrading to SecurityCenter 5.3.1. For more information about upgrading to SecurityCenter 5.3.1, refer to the SecurityCenter User Guide.

If you are using Nessus agents, SecurityCenter 5.3.1 requires Nessus Cloud or Nessus Manager 6.5 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 4.0 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.2 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter 5 API, refer to the SecurityCenter 5 API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.3.1-es5.x86_64.rpm	1e91ff19654b32f19c400fc733f73bac
SecurityCenter-5.3.1-es6.x86_64.rpm	95936f577352a404cdb949bbf6a9506d
SecurityCenter-5.3.1-es7.x86_64.rpm	638503fc3155280f4cc2229e74e97533

Resolved Items

In this release we have resolved a condition where users could see errors in the logs regarding the update of the plugin distribution. Additionally, updates were made to the security of the application. Details can be found in the Security Advisory.

PHP 5.6.21 Patch Release Notes - 5/5/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.8.2, 5.0.2, 5.1.0, 5.2.0, and 5.3.1 that updates PHP to 5.6.21.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201605.1-5.x-rh5-64.tgz	73873bdb97bf6ef60ca782edbed69955
SC-201605.1-5.x-rh6-64.tgz	40e87a74064bf7468c97d5ddbb62a1a1
SC-201605.1-5.x-rh7-64.tgz	a23c0c6aa27cba0615d67d3a716a852f
SC-201605.1-4.8.2-rh5-32.tgz	be260588964630a80b0e74af9941e2f8
SC-201605.1-4.8.2-rh5-64.tgz	77fb7426a7f5fff4a16c090f32458f06

File	MD5
SC-201605.1-4.8.2-rh6-32.tgz	c9376ecdfd4b3f7b6baf90f696323a48
SC-201605.1-4.8.2-rh6-64.tgz	5c14a21e50ef6393ebc2009a49b5479f

SecurityCenter 5.3.2 Release Notes - 5/6/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.3.2, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.3.2 supports the following direct upgrade paths:

- 4.8.1+ > 5.3.2
- 5.0+ > 5.3.2

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.1 prior to upgrading to SecurityCenter 5.3.2. For more information about upgrading to SecurityCenter 5.3.2, refer to the SecurityCenter User Guide.

If you are using Nessus agents, SecurityCenter 5.3.2 requires Nessus Cloud or Nessus Manager 6.5 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 4.0 or later. If SecurityCenter Continuous

View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.2 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.3.2-es5.x86_64.rpm	cc2fdfef591307cd2e615a46aed114b0
SecurityCenter-5.3.2-es6.x86_64.rpm	81606b15159d8ec3d9b86af8a3d02b0d
SecurityCenter-5.3.2-es7.x86_64.rpm	d337dd7b41615954bc89f3a2d1a1d70e

Resolved Items

- A Correction to help text for data expiration configuration options
- OpenSSL updated to 1.0.1t
- PHP updated to 5.6.21 (Security Advisory)

SecurityCenter 5.4 Release Notes - 7/20/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.4, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.4 includes the following new notable capabilities:

- **STIG Severity filtering** - Now filter on STIG Severity ratings of I, II, or III issues from the analysis screen or when generating a report or dashboard
- **Create Tags** - Ability to set a single tag on an asset list, query, credential management or scan policy for improve searching and scan management
- **Support for privilege escalation to CyberArk credentials** - Ability to now utilize privilege escalation capabilities when using CyberArk as your authentication record source for scanning
- **Create a report from a dashboard** - Create a report from the dashboards setting drop-down to be scheduled immediately for report creation
- **FIPS-140-2 User Interface Mode** - Configure the SecurityCenter UI to only allow users to connect to the user interface using FIPS-140-2 cryptographic modules
- **Service init exit codes** - Improved service exit code messages for troubleshooting of SecurityCenter processes

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.4 supports the following direct upgrade paths:

- 4.8.[1,2] > 5.4
- 5.[0-3] > 5.4

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.1 prior to upgrading to SecurityCenter 5.4. For more information about upgrading to SecurityCenter 5.4, refer to the SecurityCenter 5.4 User Guide.

If you are using Nessus agents, SecurityCenter 5.4 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later.

SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.4.0-es5.x86_64.rpm	afc2086f5a70d54d1cfc103736290ad7
SecurityCenter-5.4.0-es6.x86_64.rpm	2b8bc5688b9f2442d99addbbf6ee8dc4
SecurityCenter-5.4.0-es7.x86_64.rpm	26634a87b75cf73da363a6db70d7fbac

Resolved Items

Summary	Issue Number
Plugin/Feed Update links disabled with ACAS license applied	148504
Resolve the root cause for stale Dashboard Schedules	264232
Timing out when sending to a Publishing Site	271197
User update/delete fails to modify default ARC Schedule Ownership	229978
Policy Template - Basic Network Scan - Port Scan (common ports) options update	214207
Plugin id field is limited to 128 characters.	188057
Output Assets filter does not apply when added to report	265131
Vulns not remediating correctly for remote check	230171, 274078
Long asset names obscure the edit and delete controls	257168
Vulnerability analysis page Asset filter does not populate if	231425

Summary	Issue Number
immediately selected	
Value of 0 in expiration results in nightly Cleanup.php errors	233629
SecurityCenter -> LCE connection not working with LCE TLSv1.2 option enabled	248355, 233081
Change Plugin Update to Reduce the Amount of Memory Used	258478, 261386
Inconsistencies with Vulnerabilities displayed on Summary page and User responsibility page	261473
Add/Edit scan: error occurs when selecting info for Automatic Distribution	247948
Edit of Blackout Windows Target fails	263670
Section element allows additional section elements to be added	268775
Settings not imported with scan policy from 4.8.2	156014
Scan with Multiple DB Creds Only Uses First One In List	228490
Assigning a new user to ticket changes the open date field	254732
Apply Rules from recast risk rules page removes the recast label from some vulnerabilities	255225
Importing scan results can remove RECAST label for some vulnerabilities	255225
IPs in blacked out asset being scanned if other non-blacked out IPs exist	252861
User is unable to edit default rule in matrix component	232222, 266103, 253279, 267707
Clean up 'prepare repository assets' tmp directory	247916
Export to CSV default columns unchecked after first submit	231317, 262690, 262690

Summary	Issue Number
Prepare assets does not cleanup partial repo copies on copy error	247916
Asset files sometimes prepared improperly for Full Access Group #0	232424
Mobile Analysis Vulnerability Detail List - clicking on OSVDB links go to 404 Not Found	266367
Error occurs upon editing Report element with Template Chapter focus filters	37157
Address printing of Max file size in C codebase	156452
Alert user if their time zone is invalid	198926
Nessus Scanner sorting only considers first two decimal places	208109
Downloading report results by clicking the name only works once	215959
SSH communications improperly identify prompt too early in certain cases	148293
Filtering by repository zeroes IP Count	219871
Disable click listeners on active info icons	212065
Remove synchronous request for time zone from sc.model.widget.DataPointWidget::parse	203450
Confirmation boxes do not get focused for keyboards	231312
CSV report showing 'First Observed' and 'Last Mitigated' for Vuln Detail Tool	229692, 226679
Repository ID not sent to /ipInfo::GET from Browse Scan Results	214670
Quick pressing back/forward in analysis can lead to errors	231399
Event Trend tool on Event Analysis hangs	249010
"License blocked" errors corrupt Repository history files	223335
Status column displays 'undefined' on component refresh for Status Summary and Ticket List tool	232721

Summary	Issue Number
Scan fails with policy imported from 4.8.2	233323, 233281, 250214
Help Text on Data Expiration Configuration page incorrectly indicates that 0 means no expiration	233629
Classification banner obscures the last list entry on a number of pages	226099
Datagrid should handle null column values	213973
Single newlines are skipped in compliance-actual-value tag on Vuln Detail List	184773
Delete option not displayed on dashboards	221330

SecurityCenter 5.4.1 Release Notes - 11/28/2016

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.4.1, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.4.1 includes the following capability improvements:

- **Agent Error Handling** - Improved error handling for communication between Nessus Agents and SecurityCenter and Nessus Cloud
- **Report Customization** - Ability to reposition report components within a chapter or section
- **Security Improvements** - Fixes for Cross-Site Scripting and php vulnerabilities Security Advisory

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.4.1 supports the following direct upgrade paths:

- 4.8.2 > 5.4.1
- 5.[0-4] > 5.4.1

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.4.1. For more information about upgrading to SecurityCenter 5.4.1, refer to the SecurityCenter 5.4 User Guide.

If you are using Nessus agents, SecurityCenter 5.4.1 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

Note: Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.4.1-es5.x86_64.rpm	ac98f537e87c4c4afdb3df1552479a85
SecurityCenter-5.4.1-es6.x86_64.rpm	ad8e9900667b64c4bafcd1d39dd34624

File	MD5
SecurityCenter-5.4.1-es7.x86_64.rpm	1ef9792c978b229e9e22810a244f79f4

Resolved Items

Summary	Issue Number
Vulns removed/re-added in a subsequent, same-day import are lost upon rollup	260034
Incorrect column list is displayed for CSV export of VDL	262690
Get creation of differential files working with customer data	263703
Order of Filters On Vulnerability Analysis Page Causing Query Error	263713
Portuguese characters not displayed correctly in report result download prompt	266746
Blackout Windows 'Status' filter doesn't work	270466
Passing wrong labelColumn for 'Source IP Summary'	272170
Cannot successfully add Event type dashboard Pie or Bar chart if configured with Source, or Destination IP Summary tools	272170
Compliance plugin outputs not formatting correctly	274678
Running scan taking too long to appear on Scan Results	276088
Compliance check test error displays no useful information	277092
User is receiving Errors when switching to Dashboard that has been copied from a shared Dashboard	279433
IPList::union() should not care about case during IPD comparison	281079
Installer does not highlight the group where an error occurred	281569
Setup Guide - activation code validation error does not clear when corrected	281569
Add frontend validation for Host on Scanners	281569
'%' in scan names prevents browsing results	283716

Summary	Issue Number
"Last Observed" not available as a display column for CSV reports with indi scans	287289
Error loading compliance Plugin for scan with Red Hat Enterprise Virtualization Best Practices audit	287616
Add 'port' filter to drilldowns from the Vulnerability List	289421
Quickly clicking info icons in IP Summary errors	290376
Toggling between info panels causes errors	290849
Convert break tags for Remediation Summary + Others on Analysis Page	292786
Could not save filtered plugin selection in Advanced Scan Policy	292850
Sort column not being properly displayed in report	295280
URLs in cm:compliance-info not rendering properly	296747
Adjust Scan Result copy to account for copying v2 Nessus + SCAP files	297982
Users with auditor role cannot see system logs link	297992
Password field not shown when toggling an existing CyberArk credential to Password	298825
'Mitigated On' mapping to wrong column name in reports/vuln analysis	299033
Pie charts displaying </br> for List OS tool	300292
Error thrown when drilling down in Event Analysis while filtering on Not All Assets	301669
Unable to filter Analysis Vulnerabilities using Assets based on short DNS names	306524
Report definitions cannot parse contextual queries	306530
CAC User logged out for max sessions even when Session management is not enabled	309203

Summary	Issue Number
Turning off "Import Vulnerabilities" on LCE Edit does not disassociate Reps from LCE	310387
The "downloadVulns" feature is not being respected (i.e., used) in LCEStatus.php	310387
Unable to delete SSH key	252603, 297953
Set Scan Result status to Error if Repository is deleted before import	270667, 261428
Passing 'name' for exported CSV when should be passing 'pluginName'	285355, 262690
Unable to make a Scan Dependent on a Dependent scan	N/A (Internal)
XSS vulnerability in user lists	N/A (Security Fix)
XSS vulnerability in info icon popovers	N/A (Security Fix)
XSS vulnerability in matrix column and row headings	N/A (Security Fix)
XSS vulnerability found in assets - analysis asset summary tool	N/A (Security Fix)
XSS vulnerability found in assets	N/A (Security Fix)

SecurityCenter 5.4.2 Release Notes - 12/7/2016

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.4.2, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

SecurityCenter 5.4.2 supports the following direct upgrade paths:

- 4.8.2 > 5.4.2
- 5.[0-4] > 5.4.2

Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.2 prior to upgrading to SecurityCenter 5.4.2. For more information about upgrading to SecurityCenter 5.4.2, refer to the SecurityCenter 5.4 User Guide.

If you are using Nessus agents, SecurityCenter 5.4.2 requires Nessus Cloud or Nessus Manager 6.8 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 5.1 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.8 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter REST API, refer to the SecurityCenter REST API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.4.2-es5.x86_64.rpm	e0a56c00c8e08ab9a047666c45d996d5
SecurityCenter-5.4.2-es6.x86_64.rpm	dced59c257cf2565f9267b4ec4ff9f98
SecurityCenter-5.4.2-es7.x86_64.rpm	e295d67e694e2e8d2033078fc43e34a1

Resolved Items

This release fixes an issue where scans requiring DNS resolution would sometimes cause scans to complete incorrectly.

2015 Tenable Security Center

SecurityCenter 5.2 Release Notes - 12/16/2015

2015 Tenable Security Center

PHP Patch Release Notes - 2/4/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for all supported versions SecurityCenter that addresses the PHP vulnerability. This patch applies PHP 5.4.36, which is not affected, or modifies PHP 5.3.x as needed to mitigate the issue.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums for PHP Patches for SC 4.8.2

File	MD5
SC-201502.2-4.8.2-rh5-32.tgz	0673ac259e90db8d75681af5f04a4c40
SC-201502.2-4.8.2-rh5-64.tgz	8b01972998d0525ec31dfff0ec64c74b
SC-201502.2-4.8.2-rh6-32.tgz	cb8c9c6c4af75c71b909db711bffcc79
SC-201502.2-4.8.2-rh6-64.tgz	61d968c7441c4fcfae02bc17bcc9ad42

File Names & MD5 Checksums for PHP Patches for SC 4.7.1 and 4.6.2.2

File	MD5
SC-201502.2-php53-rh5-32.tgz	465c5da6a16e7caf7e7110916624b6c5
SC-201502.2-php53-rh5-64.tgz	f9dd149e395263d5592ff19d0c531ac1
SC-201502.2-php53-rh6-32.tgz	4240057a3865c50af610f717c8c85d26
SC-201502.2-php53-rh6-64.tgz	e4227104f2ff72514101bb62dfcfad3a

OpenSSL Patch Release Notes - 2/4/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for all supported versions SecurityCenter that addresses the OpenSSL vulnerability. This patch will update SecurityCenter's version of OpenSSL to 1.0.1l, which is not affected.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201502.1-rh5-32.tgz	0f74a1ec428cfc004433b7197f047f80
SC-201502.1-rh5-64.tgz	931db94496fc97f23683c5c1f81b3a32
SC-201502.1-rh6-32.tgz	5aa830cb73707a5a4fde03eea3f735a6
SC-201502.1-rh6-64.tgz	16078238a15789e3bc1006108fe81107

PHP Patch Release Notes - 3/17/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.8.2 that updates PHP to 5.4.38.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201503.1-4.8.2-rh5-32.tgz	0db54cdf7aaa87331b42705ed96bea4a
SC-201503.1-4.8.2-rh5-64.tgz	d5baa3032a250a6110d005881d16dcdc
SC-201503.1-4.8.2-rh6-32.tgz	5749448aa361c5aec5f7f7b8ac56ba70
SC-201503.1-4.8.2-rh6-64.tgz	d22886455743425031 44b43157757bd7

OpenSSL Patch Release Notes - 4/15/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for all supported versions SecurityCenter that addresses the OpenSSL vulnerability. This version bundles an updated OpenSSL library that is not affected.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201504.1-rh5-32.tgz	3f214b567df7dd91d4e9a951a2f45724
SC-201504.1-rh5-64.tgz	704705fe5c4e1cb3e48a3ab51eb77670
SC-201504.1-rh6-32.tgz	e13c0ffd61387b122c8e4057fa6b6f9d
SC-201504.1-rh6-64.tgz	579af7fde29505178da869fefef5dbd5

SecurityCenter 5.0 Release Notes - 4/30/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

SecurityCenter 5.0 represents more than 15 man-years of engineering and design work. Tenable has worked closely with over 100 of our customers to understand how we can help them succeed in their security efforts. Consequently, we have re-imagined almost everything inside of SecurityCenter 5.0, including the user experience, data optimization, reporting, and APIs. We believe these improvements are critical to ensure customers have the visibility and analysis needed to identify vulnerabilities, reduce risk, and ensure compliance.

This document describes many of the changes that are included in SecurityCenter 5.0, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades to SecurityCenter 5.0 are only supported for those users currently running SecurityCenter 4.8 or higher. Users running previous versions will need to follow the upgrade path up to at least 4.8 before attempting to upgrade to SecurityCenter 5.0. Please refer to the SecurityCenter 5.0 Upgrade Guide for information on upgrading to SecurityCenter 5.0.

SecurityCenter 5.0 only supports Nessus scanners 6.3.6 or higher. The Passive Vulnerability Scanner must be version 4.0 or higher. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, LCE 4.2 or higher is required for complete feature compatibility.

Note: with the change in API architecture (see below), all APIs created using SecurityCenter 4.x have been deprecated. Please log in to the Tenable Support Portal and access SecurityCenter 5.0 API Release Notes for additional details.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.0.0.1-es5.x86_64.rpm	6205a3de3227d2077ba9ecabd2e8d44e
SecurityCenter-5.0.0.1-es6.x86_64.rpm	7a490b08106e2fc53632d9fd9e4cfe56

5.0 New Features

- **HTML5 UI** - The entire UI has been completely transitioned to HTML5, providing a fast and flexible interface and a more rich user experience.
- **Assurance Report Cards** - These report types will allow clients to focus on measuring their success when aligning to business objectives.
- **Audit File Updates via Feed** - Tenable's extensive configuration and system hardening polices are now available as part of the feed. This includes inline Audit File configuration, which will simplify setup and allow for greater visibility in a client's environment.
- **Scan Policy Updates via Feed** - In addition to the Audit Files, SecurityCenter 5.0 also now includes scan policy templates, available as part of the feed.
- **Blackout Windows** - Blackout Windows can now be specified per asset or per IP instead of system wide. This granularity will give clients the flexibility to skip certain devices, while continuing to collect information on the rest of the hosts.
- **Data Pivoting** - SecurityCenter and SecurityCenter Continuous View clients will now be able to quickly transition to different views of data to quickly diagnose and analyze issues.
- **32 Gigabyte Repositories** - These new larger repositories will help simplify deployments and ensure all possible data can be collected.
- **Improved Disk Utilization** - SecurityCenter 5.0 now allows administrators to control the length of time of trend information stored per repository. This new granularity will ensure proper data retention and that disk space is controlled overall.
- **Increased Filtering Capabilities** - SecurityCenter 5.0 includes the ability to filter on CVSS Vector, cross-reference, and exploit frameworks for vulnerability analysis, dashboards, and reports. Event analysis has been enhanced to include Summary by Source IP, Summary by Destination IP, and Connection Summary. This increased filtering capability gives users new ways to analyze their data.
- **Trending Calculations** - In addition to the improvements in disk utilization, trend calculations will be calculated using newly created data differentials. This change will improve the initial time to calculate while ensuring the most accurate view of data over time.
- **Improved SSH Credential Support** - SecurityCenter 5.0 allows scan jobs to use up to 5 SSH username and password combinations per job. This will simplify scan management and help insure the most complete assessment of each device.

- **RESTful API** - This API update will provide a more flexible and well defined programmatic access to the SecurityCenter 5.0 application.
- **LCE Client Management Improvements** - SecurityCenter 5.0 allows greater flexibility in the creation and distribution of client polices. This new simplified method will help users ensure the greatest possible coverage overall.
- **UTF-8 Character Support** - This enables internationalization/localization for reporting.

PHP Patch Release Notes - 6/16/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.8.1 and 4.8.2 that updates PHP to 5.4.41.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201506.1-rh5-32.tgz	fe3ff5507b968082826ccca4ffa38106
SC-201506.1-rh5-64.tgz	bf669e4badbbc51fb70c90980ccb69c1
SC-201506.1-rh6-32.tgz	e07b983d6aa6e2a771e4afc66a4d4a35
SC-201506.1-rh6-64.tgz	1c1444d85eaab33f81b167175cb04c75

OpenSSL Patch Release Notes - 7/14/2015

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.6.2.2, 4.7.1, 4.8.2 that addresses the OpenSSL vulnerabilities. This version bundles an updated OpenSSL library version (1.0.1o) that is not affected.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201506.2-rh5-32.tgz	f5ae7d8d02dc7211a82cb727918baae6
SC-201506.2-rh5-64.tgz	292726fb9abbae19428821c29530737b
SC-201506.2-rh6-32.tgz	d2297a7b948c943f43c5f05f13038198
SC-201506.2-rh6-64.tgz	b43a116c22e3107f3cc94afb6396f07a

PHP Patch Release Notes - 7/20/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.8.2 that updates PHP to 5.4.43.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201507.1-4.8.2-rh5-32.tgz	3ec16979decc453f302a1f2cf79cc630
SC-201507.1-4.8.2-rh5-64.tgz	11268f0c1420647429bb6860ba672255
SC-201507.1-4.8.2-rh6-32.tgz	3d669ff82aaa0f0c51936348b15c8818

File	MD5
SC-201507.1-4.8.2-rh6-64.tgz	bda1e9eff15135dfb2aaade09d39fbb6

OpenSSL Patch Release Notes - 7/20/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.6.2.2, 4.7.1, 4.8.2 that addresses the OpenSSL vulnerabilities. This version bundles an updated OpenSSL library version (1.0.1p) that is not affected.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201507.2-4.x-rh5-32.tgz	1b36f27ede9f2456a5273b399890fae4
SC-201507.2-4.x-rh5-64.tgz	a01f077117b133a815b228e83676d7bc
SC-201507.2-4.x-rh6-32.tgz	9dea9ee20af9640c3a920907cae374d2
SC-201507.2-4.x-rh6-64.tgz	ba5e56b23b701a3df8307ccd23547f43

SecurityCenter 5.0.1 Release Notes - 7/21/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.0.1, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades to SecurityCenter 5.0.1 are only supported for those users currently running SecurityCenter 4.8.1 or higher. Users running previous versions will need to follow the upgrade path up to at least 4.8.1 before attempting to upgrade to SecurityCenter 5.0.1. Please refer to the SecurityCenter 5.0.1 Upgrade Guide for information on upgrading to SecurityCenter 5.0.1.

SecurityCenter 5.0.1 only supports Nessus scanners 6.3.6 or higher. The Passive Vulnerability Scanner must be version 4.0 or higher. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, LCE 4.2 or higher is required for complete feature compatibility.

> **Note:** with the change in API architecture (see below), all APIs created using SecurityCenter 4.x have been deprecated. Please log in to the Tenable Support Portal and access SecurityCenter 5.0 API Release Notes for additional details.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.0.1-es5.x86_64.rpm	01e98f774165813ea45c7c3f4612a13c
SecurityCenter-5.0.1-es6.x86_64.rpm	0c8afacf6db6e75572e6d50bd4d952a7

5.0.1 New Features

- **HTML5 UI** - The UI has been updated to provide a variety of improvements including the Vulnerability Analysis screen, increased visibility of recast risks, the ability to launch remediation scans from the analysis screen, launch a report from an individual scan result, and more.

- **Assurance Report Cards** - These report types will allow clients to focus on measuring their success when aligning to business objectives. The formatting and layout of the Five Cyber Critical Controls report cards have been updated.

- **CyberArk Credential Vault support** - Users can now take advantage of CyberArk's credential vault to utilize centralized credential management when performing credentialed scans.

- **Plugin database search** - Users can now use a variety of filters to search through the Plugins database.

- **Unlimited SSH and Windows credentials** - Active scans can now be configured to utilize an unlimited number of SSH and Windows credentials.
- **Security Enhancements** - Included in SecurityCenter 5.0.1 are updates to PHP version 5.6.11 and OpenSSL 1.0.1p to address security related issues in prior versions.
- **General** - Enhancements also include stability improvements, general bug fixes, and updates to the CSV report outputs.

Post-authentication Remote Command Execution Patch Release Notes - 7/24/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.6.2.2, 4.7.1, 4.8.2 that addresses the Post-authentication Remote Command Execution vulnerability.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201507.3-4.6.2.2.tgz	a59aad0e37a6277c26b93eb544eef0c5
SC-201507.3-4.7.1.tgz	48303b5f20fed21eab3417ffe32752ad
SC-201507.3-4.8.2.tgz	46b5e501b1584d1ec18716b4e532e381

Apache Patch Release Notes - 8/20/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for SecurityCenter 4.7.1 and 4.8.2 that addresses the Apache vulnerabilities.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201508.1-4.x-rh5-32.tgz	66b1ff8e795c40f5722375d032651c23
SC-201508.1-4.x-rh5-64.tgz	a141d53e9b49fb2848184f3b3f5edb25
SC-201508.1-4.x-rh6-32.tgz	103ed541fd1992e04586a22e6fd4a0b4
SC-201508.1-4.x-rh6-64.tgz	44dfa1c38921d3626d752dffa30d195f

SecurityCenter 5.0.2 Release Notes - 8/21/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.0.2, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades to SecurityCenter 5.0.2 are only supported for those users currently running SecurityCenter 4.8.1, 4.8.2, and SecurityCenter 5.0.0.1 and higher. Users running previous versions will need to follow the upgrade path up to at least 4.8.1 before attempting to upgrade to SecurityCenter 5.0.2. Please refer to the SecurityCenter 5.0.2 Upgrade Guide for information on upgrading to SecurityCenter 5.0.2.

SecurityCenter 5.0.2 only supports Nessus scanners 6.3.6 or higher. The Passive Vulnerability Scanner must be version 4.0 or higher. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, LCE 4.2 or higher is required for complete feature compatibility.

Note: with the change in API architecture (see below), all APIs created using SecurityCenter 4.x have been deprecated. Please log in to the Tenable Support Portal and access SecurityCenter 5.0 API Release Notes for additional details.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.0.2-es6.x86_64.rpm	1bd50d90e8e0197c81c4855ebaf61358
SecurityCenter-5.0.2-es5.x86_64.rpm	7ba16be87c077f257f52b927f94b7635

Bug Fixes

Summary	Support Case(s) #
Changes to Combination Assets not being saved	00150814
Updates Apache and PHP	00146245
Unable to add users via LDAP authentication	00148698
Trend lines reflect only the first Repository's data in a graph	00148448, 00143159, 00152353, 00145435, 00153584
Unresponsive Script when using the SecurityCenter UI	000147849, 00154725

Additionally, we have made several UI enhancements to improve the overall user experience.

SecurityCenter 5.1 Release Notes - 10/22/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

SecurityCenter 5 represents more than 15 person-years of engineering and design work. The Tenable SecurityCenter team worked closely with more than 100 SecurityCenter customers to understand how to best support cyber security programs and help them succeed. Based on this direct customer feedback, the SecurityCenter engineering team has re-imagined and improved almost everything in the SecurityCenter 5 solution including data optimization, reporting, APIs, and the user experience. Tenable believes these improvements will help ensure you have the visibility and analytical capabilities needed to identify vulnerabilities, reduce risk, and ensure compliance.

This document describes many of the changes that are included in SecurityCenter 5.1, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

With the release of SecurityCenter 5.1, SecurityCenter now supports importing Nessus agent results, a feature many SecurityCenter and SecurityCenter Continuous View (SecurityCenter CV) customers have requested.

SecurityCenter 5.1 also now further extends visibility into vulnerabilities and misconfigurations across the enterprise by automating the importation of scan data from Nessus agents deployed on transient or remote systems. Nessus agents deliver the detailed visibility of credentialed scans without the requirement to manage the credentials needed for traditional active scanning. Nessus agents send scan information to Nessus Cloud or Nessus Manager. SecurityCenter then automatically retrieves this information for centralized vulnerability management, analysis, and comprehensive security assurance.

Nessus agents specifically eliminate blind spots by:

- **Securing the Mobile Workforce** – You no longer have to worry about omitting assets that are not online during a vulnerability scan. Nessus agents run the scans and then upload results to Nessus Cloud or Nessus Manager when a connection is available. Results are retrieved by SecurityCenter and SecurityCenter CV from Nessus Cloud or Nessus Manager on a scheduled or on-demand basis.
- **Securing Systems on Complex or Limited Bandwidth Networks** – Nessus agents remove the challenge of performing scans over segmented or complex networks and reduce network bandwidth usage, which is important for remote facilities connected by slow networks.
- **Removing Credential Headaches** – Many organizations struggle with credential management due to regular password change policies. With Nessus agents, host credentials are no longer required, removing the need for password resets and maintenance of privileges on assets.

The list of operating systems supported by Nessus agents currently includes Windows, Mac OS X, Amazon, Debian, Red Hat, Fedora, and Ubuntu Linux variants, and this list will continue to grow. For more information about Nessus agents, please see the following resources:

- SecurityCenter 5.1 with Nessus Agent Support paper
- SecurityCenter 5.1 with Nessus Agents FAQ
- Nessus Agents FAQ
- Nessus Agents webpage
- Nessus Agents whitepaper

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

Upgrades to SecurityCenter 5.1 are only supported for SecurityCenter installations currently running SecurityCenter 4.8.1 or later. Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.1 prior to upgrading to SecurityCenter 5.1. For more information about upgrading to SecurityCenter 5.1, refer to the SecurityCenter 5.1 Upgrade Guide.

If you are using Nessus agents, SecurityCenter 5.1 requires Nessus Cloud or Nessus Manager 6.5 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 4.0 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.2 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter 5 API, refer to the SecurityCenter 5 API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.1.0-es5.x86_64.rpm	0870e2432421457b6a900f6e2988256b
SecurityCenter-5.1.0-es6.x86_64.rpm	dda129f236ee3a1578bafdb49231fe94

SecurityCenter 5 Solution Features

- **HTML5 UI** - The entire UI has been completely transitioned to HTML5, providing a fast and flexible interface and a more rich user experience.
- **Assurance Report Cards** - These report types allow you to focus on measuring your success when aligning to business objectives.
- **Audit File Updates via Feed** - Tenable's extensive configuration and system hardening polices are now available as part of the feed. This includes inline Audit File configuration, which simplifies set up and allows for greater visibility into your environment.
- **Scan Policy Updates via Feed** - In addition to the Audit Files, SecurityCenter 5 also now includes scan policy templates, available as part of the feed.
- **Blackout Windows** - You can now specify blackout windows per asset or per IP address instead of system-wide. This granularity gives you the flexibility to skip certain devices, while continuing to collect information on the rest of the hosts.
- **Data Pivoting** - With SecurityCenter and SecurityCenter Continuous View, you can now quickly transition to different views of data to quickly diagnose and analyze issues.
- **32 Gigabyte Repositories** - New, larger repositories help you simplify deployments and ensure data can be collected.
- **Improved Disk Utilization** - SecurityCenter 5 now allows administrators to control the length time of trend information is stored per repository. This new granularity ensures proper data retention and helps control overall disk space utilization.
- **Increased Filtering Capabilities** - SecurityCenter 5 includes the ability to filter on CVSS vector, cross-reference, and exploit frameworks for vulnerability analysis, dashboards, and reports. Event analysis has been enhanced to include Summary by Source IP, Summary by Destination IP, and Connection Summary. This increased filtering capability gives you new ways to analyze your data.

- **Trending Calculations** - In addition to the improvements in disk utilization, trend calculations are calculated using newly created data differentials. This change improves the initial time to calculate while ensuring the most accurate view of data over time.
- **RESTful API** - API updates provide more flexible and well-defined programmatic access to the SecurityCenter 5 application.
- **LCE Client Management Improvements** - SecurityCenter 5 provides greater flexibility when creating and distributing client polices. This new, simplified method helps ensure the greatest overall possible coverage.
- **UTF-8 Character Support** - This enables internationalization and localization for reporting.
- **Nessus Agents** - Automated import of scan data from Nessus agents.
- **CyberArk Support** - An option for managing scanning credentials.
- **Unlimited Credentials** - Removed the restrictions on the number of SSH and Windows credentials that can be added to a scan.

Resolved Items

Summary	Issue Number
SQL Windows Authentication does not work.	162822
Popovers Behave Unreliably in Low Resolution Web Browsers	151968
Delete Recast/Accept Risk Rules	168462
Dependent Scan Configuration Produces UI Errors	167589
LDAP Query Asset - Search String limitation	162133
"Send to Report" controlled by Role setting "Upload Nessus Scan Results"?	159458
Possible Memory Leak - Excessive Memory Consumption	153403
UI Allows Editing of Scans in Other Groups	159225
Normalized Event Summary Time Is Offset by Several Hours	140355
Remediation Scans are Broken: "getTemplateLookups is not a function"	156519
Error Attempting to Edit Selected Audit File	140850

SecurityCenter 5.2 Release Notes - 12/16/2015

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 5.2, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

New Features and Enhancements

Based on customer feedback and Tenable's own rigorous internal testing process, the latest release of SecurityCenter 5.2 includes more than 180 updates, enhancements, and resolved issues.

The new SecurityCenter 5.2 release also includes the following new notable capabilities (previously available in SecurityCenter 4.8, now also available in SecurityCenter 5.2):

- **Quickly rearrange dashboard components:** SecurityCenter 5.2 now allows you to use drag and drop to quickly and easily rearrange dashboard components on the fly.
- **Fast, flexible Log Correlation Engine (LCE) searches:** SecurityCenter 5.2 now allows you to type in filters as text strings when building queries and searching across event and vulnerability information in LCE.
- **Allow Users to share objects with a Group:** SecurityCenter 5.2 now allows at the time of creation or when editing a group the ability to share polices, assets, reports, etc.

Before You Upgrade

If you are planning an upgrade from SecurityCenter 4.x, due to the many enhancements and changes made in the SecurityCenter 5 solution, Tenable strongly encourages you to install and test the latest version of SecurityCenter in a pre-production environment prior to upgrading in your production environment to ensure the new workflows and enhancements are compatible with your current workflows. To receive an evaluation key that will allow you to install SecurityCenter in a pre-production environment for evaluation, log in to the Tenable Support Portal and click "Activation Codes". Under SecurityCenter, you will see a link to download a demo key for the SecurityCenter 5 solution.

Upgrade Notes

Upgrades to SecurityCenter 5.2 are only supported for SecurityCenter installations currently running SecurityCenter 4.8.1 or later. Installations running previous versions of SecurityCenter 4.x must upgrade to at least 4.8.1 prior to upgrading to SecurityCenter 5.2. For more information about upgrading to SecurityCenter 5.2, refer to the SecurityCenter Documentation.

If you are using Nessus agents, SecurityCenter 5.2 requires Nessus Cloud or Nessus Manager 6.5 or later. If you are not using Nessus agents, SecurityCenter requires Nessus Scanner 6.3 or later. SecurityCenter requires the Passive Vulnerability Scanner 4.0 or later. If SecurityCenter Continuous View uses the Log Correlation Engine (LCE) for log processing, SecurityCenter requires LCE 4.2 or later for complete feature compatibility.

> **Note:** Due to changes in API architecture, all APIs created using SecurityCenter 4.x have been deprecated. For more information about SecurityCenter 5 API, refer to the SecurityCenter 5 API Documentation.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-5.2.0-es5.x86_64.rpm	8bd224bf21c7aacce347c83c57debc48
SecurityCenter-5.2.0-es6.x86_64.rpm	8e4b01fdaf2cc87e691299c983f2dc04

Resolved Items

Based on customer feedback and its own rigorous internal testing process, this release includes more than 180 updates and resolved issues. Below is a brief description of the most significant items resolved in the Security Center 5.2 release:

Summary	Issue Number
CSV Report Errors with Events	187002
Dashboard Components errors when editing asset attributes	140417
Reports not showing mitigated data correctly	183942, 171767
Browser back button does not work correctly when setting multiple filters on vulnerability screen	145781

Summary	Issue Number
Error when Creating Asset with Plugin ID	179103
Error when modifying report columns and headers can cause the order to become incorrect	166434
Custom report error when generated by saved query, incorrectly reverts to vuln summary tool	156582
LCE Clients page: Unable to get property "id" of undefined or null reference	158283

2014 Tenable Security Center

2014 Tenable Security Center

SecurityCenter 4.8 Release Notes - 3/20/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 4.8, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.7.1 and later. Users upgrading from 4.7 and earlier must first perform an upgrade to SecurityCenter 4.7.1 before attempting to upgrade to version 4.8. Please refer to the SecurityCenter 4.7 Upgrade Guide for information about upgrading to SecurityCenter 4.7. Information about upgrading from SecurityCenter 4.7.1 is available in the SecurityCenter 4.8 Upgrade Guide.

SecurityCenter 4.8 only supports Nessus scanners 5.x or later. The Passive Vulnerability Scanner must be version 4.0 or higher. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes and LCE 4.2.x for complete feature compatibility.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.8.0-es5.i386.rpm	[9de46a946a88bdcfffe0e0f0a3528fc4]
SecurityCenter-4.8.0-es5.x86_64.rpm	[1e2acf576960e3e2f27c5f551d34c063]
SecurityCenter-4.8.0-es6.i386.rpm	[9411a5c135472b9876f76139417c693d]
SecurityCenter-4.8.0-es6.x86_64.rpm	[735887007534a0ba32382b57259c6aeb]

4.8 Features

User Model

There has been a complete revamp of the user model within SecurityCenter. There is no longer a hierarchal mode of creating users and managers. The user model now follows the more common "grouping" method of creating and managing users.

Groups are now used to define what security data (vulnerabilities, events, etc.) people have access to. Roles and permissions are used to define what they can do with it. Below is a brief comparison of some functionality between 4.8 and previous versions:

4.7 and Previous Releases	4.8
The OrgHead account needed to be shared to provide full management access.	User-Group relationships allow an unlimited number of users full access to both users and objects across the organization.
The user hierarchy is problematic as it cannot be altered after user creation.	User hierarchy is replaced by user groups. Users may be moved between groups.
Managers cannot manage "all" users due to the hierarchy. A manager has no visibility into to users created by the OrgHead account or other managers.	User hierarchy is replaced by groups, and any user with "Manage Users" access to the group will be able to manage all users within that group. So, the "SecurityManager" can create a group, assign users to it, and any other users who have "Manage Users" access to that group will also be able to manage those users, regardless of who created them.
Neither OrgHead nor managers can manage scans or reports created by other users.	Any user with "Manage Objects" access to a group will be able to edit/delete/use any object created by any user who belongs to that group.
Complex asset calculations due to hierarchy and having to compute for every user.	Asset calculations are done for the group, rather than for individual users. So, if you had 100 users in an organization and they were divided in 3 groups, asset calculation is run only 3 times versus 100.

HTML5

In SecurityCenter 4.8, we have continued to migrate more of the application over from Flex to HTML5. The big addition was the introduction of the "Analysis" screen into the HTML app. This also allowed us to enable the drill-down from the dashboard.

There are a lot of changes from a look and feel perspective as well as workflow on the new "Analysis" page. This release is intended to introduce users to the more streamlined, easier to use SecurityCenter.

Combination Asset Support

In previous versions of SecurityCenter, users had the ability to create pretty powerful asset lists dynamically using a number of different methods. However, there was no way for them to merge multiple dynamic asset lists into a single dynamically updated asset list. In 4.8, we have added this functionality.

For example, you can create one asset list that covers Windows servers and a second asset list that contains Windows workstations. You can create a single dynamic asset list that contains those two assets. As each of the individual asset lists gets updated, so does the parent.

Combination Filtering

In 4.8 we have considerably enhanced filtering capabilities. Users now have the ability to apply set logic against multiple assets. For example, while on the "Analysis" screen you are now able to perform a filter that essentially does: "I want to look at all the vulnerabilities that are in Asset A and Asset B and are not in Asset C".

Defining User Responsibility

A new feature in this release is the introduction of defining "User Responsibility". This will allow managers to associate an asset with a user. At that point, the user can configure dashboards or reports that are based solely on the IPs that they are responsible for.

Updated method for handling Database Credentials

In previous versions of SecurityCenter, when defining a scan that required the need to include database credentials, you needed to define that in each scan policy you created. In other words, the credentials you needed for scanning a database was not being serviced by the Credentials portion of the application. In 4.8, this is no longer the case.

Support for PCRE in Dynamic Asset Lists

In 4.8, we have added the support for Perl Compatible Regular Expression (PCRE) when defining dynamic asset lists. Previously we only supported POSIX, which does not allow for setting a negative operator. Now with the addition of PCRE, support for this has been added.

Updated communication between PVS and SecurityCenter

In SecurityCenter 4.8, we have updated how PVS and SecurityCenter communicates. These changes will allow for better management of PVS. Due to this change, all attached PVS scanners must be of version 4.0 or higher.

Bug Fixes

- IP Ratio Matrix breaks template
- Fixed an issue with prepare_rep_assets which is causing asset list calculations to show zero.
- Resolved an issue when CSV Reports are disabled after editing copy.
- Fixed an issue where CSV reports are missing lines, every 5000 lines it drops a line.
- Resolved the issue that generated the follow error: "Dashboard component #xxx not found. Unable to retrieve Component #xxx".
- Fixed the issue where a user could not send a Customer Dashboard to a report.
- Numerous other fixes.

SecurityCenter 4.8.1 Release Notes - 5/29/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 4.8.1, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.8. Users upgrading from 4.7 and earlier must first perform an upgrade to SecurityCenter 4.8 before attempting to upgrade to version 4.8.1. Please refer to the SecurityCenter 4.8 Upgrade Guide for information about upgrading to SecurityCenter 4.8. Information about upgrading from SecurityCenter 4.8 to 4.8.1 is available in the SecurityCenter 4.8.1 Upgrade Guide.

SecurityCenter 4.8.1 only supports Nessus scanners 5.x or later. The Passive Vulnerability Scanner must be version 4.0 or higher. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes and LCE 4.2.x for complete feature compatibility.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.8.1-es5.i386.rpm	[be84235d7c3836e0f931fd6395f55dae]
SecurityCenter-4.8.1-es5.x86_64.rpm	[aac1c12443978cb2c54ae3405bf70df1]
SecurityCenter-4.8.1-es6.i386.rpm	[de5786cde8fcba48e7bc9b7d95b88186]
SecurityCenter-4.8.1-es6.x86_64.rpm	[7d377cf6f3926f6ae7763e5db4e78eef]

4.8 Features

Changes to Nessus Enterprise Cloud (formerly Perimeter Service) scan settings – A number of changes were made to streamline SecurityCenter and Nessus communication (changes are only applied to communication within the Nessus Enterprise Cloud). Some of these changes include:

- Larger scan chunks sent to scanner
- Out of service threshold increased
- Status polling interval increased

PCRE support for vuln text – Full PCRE support is now available when filtering on vulnerability text. This can be used in all areas of SecurityCenter where vulnerability queries are used including Vulnerability Analysis, Dashboard, Reporting, and Alerts.

Performance improvements for managing Reports and Dashboards – As the number of viewable dashboards and reports increased, the load time for the dashboard and report management pages became too long. Changes were made in the communication to significantly speed up those processes by only passing back the full query definitions for a report or dashboard when an edit was performed as opposed to on initial load.

Implement .k5login privilege escalation – To support new Nessus functionality, we have added the ability for a user to select ".k5login" as an option in the privilege escalation drop-down for SSH credentials.

Upgrade to PHP 5.4.28 – To address security issues within PHP, we have upgraded PHP to version 5.4.28.

Bug Fixes

- Resolved the issue where a rollover scan would continually copy itself over causing multiple scan jobs to execute over time.
- Addressed an issue with tag selection in the "Output Asset" filter.
- Fixed a bug that listed incorrect users within the User Responsibility Summary.
- Resolved the issue where the "Perform PCI DSS Analysis" checkbox is not enabled in the UI when adding a PCI DSS Scan policy template.
- Addressed the issue where a user was not able to log in to the HTML application using a CAC card.
- Fixed the bug that caused a PVS offline update to fail due to not being registered.
- Fixed the incorrect authentication settings for MSSQL Server
- Addressed the issue where certain credentials were being stored in the clear in the sc4-configuration.txt file.
- Resolved a user model bug in which a user is unable to delete an asset that is assigned as a "Responsible Asset" to a deleted user.
- Fixed a bug in the HTML application that would not allow a user to use the "combination of" functionality when filtering on an asset.
- Addressed the general error that was thrown stating "Please specify the list of assets" in the HTML application.
- Resolved the issue when trying to send a dashboard to a report and the vulnerability bar would not render.
- Fixed the bug where a filter that was applied on the "Assets" page persisted in filters on the "Analysis" page.
- Numerous other fixes.

SecurityCenter 4.6 - 4.8 OpenSSL "ChangeCipherSpec" man-in-the-middle (MiTM) Vulnerability Patch Release Notes - 6/10/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The SecurityCenter patch for the OpenSSL "ChangeCipherSpec" man-in-the-middle (MiTM) Vulnerability (CVE-2014-0224) is now available for SecurityCenter versions 4.6.2.2, 4.7.0, 4.7.1, 4.8.0, 4.8.1. Users are encouraged to update immediately.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "OpenSSL-1.0.1h->os>->arch>.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: tar zxf ./OpenSSL-1.0.1h-rh5-32.tgz

Run the install.sh: ./install.sh

File Names & MD5 Checksums

File	MD5
OpenSSL-1.0.1h-rh5-32.tgz	[39ff3b319674413c6ef2835ef58cb036]
OpenSSL-1.0.1h-rh5-64.tgz	[59876b23e269a01cd3dd44ca713df87b]
OpenSSL-1.0.1h-rh6-32.tgz	[34841a0a924947456b9ba7aed40605a2]
OpenSSL-1.0.1h-rh6-64.tgz	[c304eec1b5b0d636dd3315ca93744801]

PHP/Apache Vulnerability Patch Release Notes - 7/16/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The SecurityCenter patch for the PHP/Apache vulnerabilities (CVE-2014-3515, CVE-2014-0098) is now available. For CVE-2014-0098 (Apache HTTP Server), patches are provided for SC 4.8.1, SC 4.7.1, and SC 4.6.2.2. The SecurityCenter 4.8.1 patch also fixes CVE-2014-3515 (PHP). Users are encouraged to update immediately.

Customers with SecurityCenter 4.6.x and 4.7.x that wish to apply a patch for the PHP related vulnerabilities can upgrade to SecurityCenter 4.8.1 and apply the patch mentioned above.

Note that this patch will re-apply the patches for OpenSSL as noted in TNS-2014-02 and TNS-2014-03.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
sc4.8.1-rh6-64.tgz	4ad4fb7bee4546d4c3a59b3ae3da39a6
sc4.8.1-rh6-32.tgz	7a9b66ac070bb322d9eb9127beedab57
sc4.8.1-rh5-64.tgz	003fd53de9d56568d3c29e08c93bcb90
sc4.8.1-rh5-32.tgz	639d867aee00d05f10d71c35ea5683bc
sc4.7.1-rh6-64.tgz	0c23ec8403b4f865953eb5aca6248f16
sc4.7.1-rh6-32.tgz	31e802c05658d9e363174cdaca5461ac
sc4.7.1-rh5-64.tgz	d88d8e5842122da166fcb45ccda01233
sc4.7.1-rh5-32.tgz	3e9f009924e692aeae0e795c74b17a2f
sc4.6.2.2-rh6-64.tgz	4df5e9904c58a881fa01ca5ac6c52dde
sc4.6.2.2-rh6-32.tgz	c014d0258a8af365e5cd609741ea8aab
sc4.6.2.2-rh5-64.tgz	fd160d7edb47a00a015624048b941583
sc4.6.2.2-rh5-32.tgz	ca22c43ca32b9bc6698c3cc2300ef8f7

OpenSSL Patch Release Notes - 8/21/2014

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This patch will update SecurityCenter's version of OpenSSL to 1.0.1i.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
OpenSSL-patch-Aug2014-rh5-32.tgz	a734a584729cd34222979070443a4f9a
OpenSSL-patch-Aug2014-rh5-64.tgz	75da02df97ddae68a33e274c46344aa0
OpenSSL-patch-Aug2014-rh6-32.tgz	8b8cf69e94e2ac14bf3d41eab04437e5
OpenSSL-patch-Aug2014-rh6-64.tgz	3c007c799636763c56ae2fedaa063882

OpenSSL Patch Release Notes - 11/7/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Tenable has released a patch script for all supported versions SecurityCenter that addresses the OpenSSL vulnerability. This patch will update SecurityCenter's version of OpenSSL to 1.0.1j.

For more information, see the Security Advisory.

To patch SecurityCenter, download the appropriate patch to the SecurityCenter host. Files are named "--.tgz". We recommend you put it in /tmp or its own folder.

Untar patchfile: # tar zxf ./--.tgz

Run the install script: # ./install.sh

File Names & MD5 Checksums

File	MD5
SC-201411.1-rh5-32.tgz	14b0fcfe090fc33d5dd6eba8170ccb1e
SC-201411.1-rh5-64.tgz	f0cf7cad17aa318da80f0307f1102ba5
SC-201411.1-rh6-32.tgz	7f3e64f1ff11daef718b2ce2f40c9520
SC-201411.1-rh6-64.tgz	bd04d683d1fa1a7c24edee71eb1c62f5

SecurityCenter 4.8.2 Release Notes - 12/16/2014

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 4.8.2, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.8. Users upgrading from 4.7.x and earlier must first perform an upgrade to SecurityCenter 4.8 before attempting to upgrade to version 4.8.2. Please refer to the SecurityCenter 4.8 Upgrade Guide for information about upgrading to SecurityCenter 4.8. Information about upgrading from SecurityCenter 4.8 to 4.8.2 is available in the SecurityCenter 4.8.x Upgrade Guide.

SecurityCenter 4.8.2 only supports Nessus scanners 5.x or later. The Passive Vulnerability Scanner must be version 4.0 or higher. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes and LCE 4.2.x for complete feature compatibility.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.8.2-es5.i386.rpm	b9187b21312e602a6d79a6a417f32b31
SecurityCenter-4.8.2-es5.x86_64.rpm	fd27b5508e1905c2ac7c3cf7ef90fc27
SecurityCenter-4.8.2-es6.i386.rpm	4b30b9503337dda013dcad91a02660b4
SecurityCenter-4.8.2-es6.x86_64.rpm	75db6fd8f355809b2e1dfafe3931b702

4.8.2 New Features

- **Report PDF table of contents** - Generated reports now contain bookmarks within the PDF for easier navigation through large reports.
- **Report name contains scan name** - When a scan completes and is configured to generate a report, that report now includes the scan name from which it was generated.
- **Larger file uploads** - On new installations; a larger default file upload setting of 500MB is used.

Bug Fixes

- Bug fixed - A 404 Not Found error when uploading a license key or other text files
- Bug fixed - SecurityCenter error upon Nessus 6 policy import
- Bug fixed - where SecurityCenter becomes unresponsive when selecting: Scanning - Scans - Owner (and choosing a name from the drop-down)
- Bug fixed - the "address" filter in Scan Zones not behaving as expected when viewing CDIRs

2013 Tenable Security Center

2013 Tenable Security Center

SecurityCenter 4.6.2 Release Notes - 2/7/2013

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 4.6.2, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.2.0 and later. Users upgrading from 4.0.x must first perform an upgrade to SecurityCenter 4.2 or 4.4 before attempting to install version 4.6. Please refer to the SecurityCenter 4.2 Upgrade Guide or SecurityCenter 4.4 Upgrade Guide for information about upgrading to SecurityCenter 4.2 or 4.4. Information about upgrading from SecurityCenter 4.2.0 and later is available in the SecurityCenter 4.6 Upgrade Guide.

SecurityCenter now only supports Nessus scanners 4.2 or later. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.6.2.2-es5.i386.rpm	[8e788a82bacd5249084ca5cd29f90e74]
SecurityCenter-4.6.2.2-es5.x86_64.rpm	[29b5809d410c895b26b7eae8caf7eb8f]
SecurityCenter-4.6.2.2-es6.i386.rpm	[5461c400aa17b3eefeffcbfe63e94851]
SecurityCenter-4.6.2.2-es6.x86_64.rpm	[c9d8eb8fbe55e2bb80783e15565bb234]
LCEManager-4.6.2.2-es5.i386.rpm	[b626e21b2677cab24c1099b35301c248]
LCEManager-4.6.2.2-es5.x86_64.rpm	[7d5929e3be0297edc1643abd5582dfac]
LCEManager-4.6.2.2-es6.i386.rpm	[599a53170b448a92c947a9d2dc62dbad]
LCEManager-4.6.2.2-es6.x86_64.rpm	[fa6daa6a89cf013e27c8769a62069fc6]

Changes and New Features

General

- **Publishing Sites** – This new feature allows users to move reports from SecurityCenter to a third-party system. Users can configure the reports to be published automatically, or can manually push the report when needed. The following two types of publishing methods are introduced in SecurityCenter 4.6.2:
  - **CMRS** – This publishing is used strictly to support a particular project, and will export the new ARF and ASR reports. This method uses WS-Notify and is specifically designed to work for that system.
  - **HTTP Publishing** – This publishing is what all other users can use to publish any report that SecurityCenter can produce today. It uses a simple HTTP POST and utilizes BASIC Auth.

Management

- **Repository Splitting** – For very large customer deployments, there are times when Repository size limits hits its 4GB threshold. SecurityCenter 4.6.2 introduces a command-line tool that allows users to split a portion of their Repository, and move the data into a new Repository. The user will have to go through Tenable Support in order to get access to this tool.
- **Links to Dashboard/Reporting blog** – To help new or uninformed users with all the content provided by Tenable, we have introduced links that point users to canned Dashboard and Report templates posted on the Tenable blog.
- **Enabled v2 data download by default on new installs** – On new installs we now by default only download Nessus v2 data. This is a more efficient means for the SecurityCenter to import scan results from Nessus. There is a global setting to enable v1 and/or disable v2. Under most circumstances, all users are recommended to disable v1 and only offer v2 options after an upgrade.

Reporting

- The Reporting/Scanning tab settings in the Admin interface offers the option to enable or disable a variety of reporting types that are encountered and needed only in specific situations.
- **Generate an ASR report** – This feature provides the ability to generate an Assessment Summary Report (ASR) (for use only projects that require this reporting format)
- **Generate an ARF report** – This feature provides the ability to generate an Asset Reporting Format report (ARF) (for use only projects that require this reporting format)
- **Define operational attributes for reports** – SecurityCenter 4.6.2 provides the ability to define operational attributes that are used to help define the content in an ARF/ASR report. This feature allows you to generate a report based on those attributes. (for use only projects that require this reporting format)
- **Generate a CyberScope report** – This feature provides the ability for SecurityCenter to generate a CyberScope/LASR report directly from the application. Previously, the xTool utility was needed to connect to SecurityCenter, pull the data, and generate the report.

Bug Fixes

- Fixed an issue where a user could not select or de-select an Asset that was in an Asset Group
- Resolved the issue where, in certain circumstances, deleting a Repository did not re-calculate IP count against the license.
- Fixed an issue that, while in LCE mode, the Load Template form contained a repository listbox.
- Many other minor improvements and bug fixes.

4.6.2.1 (2/18/2013)

This release fixes various bugs.

4.6.2.2 (4/10/2013)

Changes and New Features

- Importing Vulnerability data from LCE - SecurityCenter has added the ability to import vulnerability data that has been derived via logs through the Log Correlation Engine. This feature will not be usable until the release of LCE v4.2.
- SecurityCenter to Nessus communication compression - The SSL communication between SecurityCenter and Nessus will now be compressed. In the past, the transfers of scan results were sent uncompressed. Compressing data aids in environments with slow links between the SecurityCenter and scanners.
- Support for Palo Alto Compliance check - Nessus has added the ability to scan Palo Alto firewalls. This addition allows for the checks to be managed from the SecurityCenter as well.
- Optimization of Dynamic Asset List calculation - Enhancements have been made to improve the performance when creating Dynamic Asset Lists.
- Upgrade of Apache - There were vulnerabilities found in the version of Apache that was running on the previous versions of SecurityCenter. While SecurityCenter was not using any of the vulnerable modules, we upgraded to the latest version of Apache to stay current.

Bug Fixes

- Fixed the issue of stale scan jobs remaining in the UI, even after the job has been killed.
- Fixed the bug where DNS and LDAP assets where not being updated nightly.
- Resolved the issue of duplicate tabs on the dashboard.

- Removed the errors in the admin log when creating a new Orghead
- Addressed the issue when creating a report with an Iterator is launched via a scan and it is not using the IPs from the scan result.
- Fixed the issue where report filters in elements under Sections, Groups, or Iterators would become corrupt after it was launched via scan.
- Resolved the issue when editing a matrix cell on the dashboard caused the following error to appear "<x> correction(s) required. Condition: A matching condition already exists in the definition".
- Fixed the bug that occurred when editing an RTF report added a report image to the cover page when it should not have.
- Re-added the "Total IPs" to the scan results page. This was mistakenly removed in the previous release.

SecurityCenter 4.7.0 Release Notes - 8/29/2013

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 4.7, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.2.0 and later. Users upgrading from 4.0.3 must first perform an upgrade to SecurityCenter 4.2 or 4.4 before attempting to upgrade to version 4.7. Please refer to the SecurityCenter 4.2 Upgrade Guide or SecurityCenter 4.4 Upgrade Guide for information about upgrading to SecurityCenter 4.2 or 4.4. Information about upgrading from SecurityCenter 4.2.0 and later is available in the SecurityCenter 4.7 Upgrade Guide.

SecurityCenter 4.7 only supports Nessus scanners 4.2 or later. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes and LCE 4.2.x for complete feature compatibility.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.7.0-es5.i386.rpm	9fa40f1b694d19ce9564155ae251b24b
SecurityCenter-4.7.0-es5.x86_64.rpm	6bd4b9c724df81196b5f8ce2d246493b
SecurityCenter-4.7.0-es6.i386.rpm	0a2fcb51ff05910e8caf919d1c4fafdf
SecurityCenter-4.7.0-es6.x86_64.rpm	0ad237e3b54dce76dc5e2301db3d2599

Changes and New Features

General

- New SecurityCenter feed will automatically update Dashboard, Report, and Asset templates as well as remediation lists. The latest audit plugins will become usable in SecurityCenter as soon as they are released in Nessus
- Ability to view Solaris servers when using the "List Software Tool"
- Added matrices to reports
- Sortable columns when dealing with Event data

Mobile Devices

- Scan, import, and summarize mobile device vulnerability data using a number of analysis tools
- Drill-down to get to mobile device vulnerability details
- Filter mobile data
- Report on mobile data
- Create dashboard components featuring mobile data
- Save, load, and manage mobile queries
- Synch mobile repositories across different SecurityCenters
- Import/export a mobile repository
- Pull mobile device vulnerability information from Apple MDM, ActiveSync, and Good MDM

SCAP

- Download the raw OVAL/XCCDF results files after a scan completes
- Upload OVAL/XCCDF audit files as a new type
- Filter on an OVAL/XCCDF audit file
- Run a scan with OVAL/XCCDF files exactly like current audit files and browse the results

Risk Management

Remediation Report

- Remediation driven vulnerability analysis tool (i.e., "Upgrade to the latest version of Google Chrome") including the impact of the fix
- Show vulnerabilities remediated, risk reduced, MS Bulletins remediated, CVEs remediated, and number of hosts affected
- Analysis tool can drive dashboards and reports

Accept/Recast Risk

- Ability to manage accepted and re-casted risk rules as a user
- Set an expiration date for Accept Risk rules

Number of days it took to mitigate a vulnerability

- The "First Discovered" date/time will be modified to be the most recent first discovery, as opposed to the actual discovery
- The matrix will now allow mitigated vulnerability data
- A new filter is created to view the amount of time it took for a vulnerability to become mitigated

Templates

Dashboard Templates

- Add a set of dashboard components from a dashboard collection template
- Add dashboard components from a list of pre-defined single component templates
- Select dashboard templates using operational categories
- Filter dashboard templates using tags

- Quickly add tabs and components
- Create custom dashboard components from scratch within the new template interface
- Search dashboard templates
- View the details of dashboard templates
- Configure dashboard templates to target specific assets/repositories/IP addresses

Report Templates

- Create a report using Tenable supplied templates
- Select report templates using operational categories
- Filter report templates using tags
- Create custom reports from scratch within the new template interface
- Search report templates
- View the details of report templates
- Configure report templates to target specific assets/repositories/IP addresses

Asset Templates

- Create an asset using Tenable supplied templates
- Select assets using operational categories
- Filter asset templates using tags
- Create custom assets from scratch within the new template interface
- Search asset templates
- View the details of asset templates

Scanning

- Blackout windows will now stop scans that are running when the blackout window starts. Previous functionality only prevented starting new scans during the window
- The stopped scan will turn into a rollover scan. The rollover scan will be configured to restart 24 hours after the stopped scan initially started or may be manually be started at an earlier time

Reporting

- Improved styling
- Ability to export dashboards into a report
- Ability to create a report from an individual scan result using an existing template

Bug Fixes

- Publishing Sites can be duplicated on the Distribution Tab of DISA ARF and DISA ASR Reports.
- Authentication: Editing users using certificate authentication fails after password length restrictions are changed.
- Web app scan against virtual hosts not sending DNS names when default scan zone is used.
- Bar chart y-axis label incorrect for List Services output in reports.
- System->Keys: Error Code: 146 Unable to add SSH key when attempting to add an RSA or DSA key to SecurityCenter with an empty comment.
- DNS Asset Detail shows IPv4 addresses under IPv6 rep when IPv6 rep is defined with very large range.
- Selecting many Organizations when adding/editing publishing sites does retain all selections.

SecurityCenter 4.7.1 Release Notes - 10/16/2013

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 4.7.1, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.2.0 and later. Users upgrading from 4.0.3 must first perform an upgrade to SecurityCenter 4.2 or 4.4 before attempting to upgrade to version 4.7. Please refer to the SecurityCenter 4.2 Upgrade Guide or SecurityCenter 4.4 Upgrade Guide for information about upgrading to SecurityCenter 4.2 or 4.4. Information about upgrading from SecurityCenter 4.2.0 and later is available in the SecurityCenter 4.7 Upgrade Guide.

SecurityCenter 4.7 only supports Nessus scanners 4.2 or later. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes and LCE 4.2.x for complete feature compatibility.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.7.1-es5.i386.rpm	e5d3cb3910a7b6ffcb11518cc3fb4bfc
SecurityCenter-4.7.1-es5.x86_64.rpm	51c9501494dd260d70700400ac0d0f3b
SecurityCenter-4.7.1-es6.i386.rpm	72da4376dcb4c70af86fb432038b9fa6
SecurityCenter-4.7.1-es6.x86_64.rpm	77c031f07debe047b40482f76c31dddf

Changes and New Features

- Updated Remediation Summary tool in Vulnerability Analysis to provide a more descriptive resolution
- Modified "is equal to" operator for Dynamic Asset clauses to be exact match instead of contains
- Updated font for PDF reports

Bug Fixes

- Fixed issue where Dashboards would become corrupt after deleting a Report created from a Dashboard
- Fixed issue where editing a Report created from a Dashboard failed
- Fixed issue with filtering using LDAP Query Assets
- Fixed issue with adding a Report from the Scan Results page using a saved Query
- Fixed issue with browsing vulnerability results with an Asset filter
- Fixed issue with calculating ratios in Matrix components for Reports
- Fixed vulnerability import error when parsing compliance check names

- Fixed issue with retaining LCE Event Vulnerability configuration on upgrade
- Re-enabled host ping settings (plugin id #10180) by default on Scan Policy creation
- Updated 'upload_max_filesize' php directive to 300 MB to accommodate Offline Plugin updates
- Fixed intermittent GUI error on logout

2012 and Earlier Tenable Security Center

SecurityCenter 4.2.0 Release Notes

SecurityCenter 4.4.0 Release Notes - 4/17/2012

SecurityCenter 4.6.0 Release Notes - 12/4/2012

Security Center 3.0.4 Release Notes

Security Center 3.0.5 Release Notes

Security Center 3.0.6 Release Notes

Security Center 3.0.6 Hotfix01 Release Notes

SecurityCenter 3.2 Release Notes

SecurityCenter 3.2.1 Release Notes

SecurityCenter 3.2.2 Release Notes

2012 and Earlier Tenable Security Center

SecurityCenter 3.0.2 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features in 3.0.2

- Each user now automatically has an additional asset group named "All Assets". This asset group is an aggregate of each of their assigned assets. It is also the default asset group used for filtering. This allows every user to see all of their security issues, even if they have been assigned discrete asset ranges.
- Support for Nessus 3 .nbin files was added. Nessus 3 includes the ability to scan a host with a different type of plugin with an '.nbin' extension. These plugins are pre-compiled and only run on Nessus 3.

Major Bug fixes in 3.0.2

- SSH keys for UNIX local checks are correctly passed to the Nessus scanners.
- In certain circumstances there were issues downloading large reports using Internet Explorer over SSL. These issues have now been resolved.

- Creation of customer names, static, or dynamic asset lists now includes the use of hyphens and under-scores.

Other Minor Issues Resolved

There were many other items that were resolved to correct the program or to accommodate comments on usability of the system.

Security Center 3.2.3 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Special Note Regarding Security Center Plugins Updates:
As noted in the "SC Security & Auditing" section below, Security Center plugins updates for both Nessus and PVS have enhanced security which includes a secure channel for downloading the updates. If Security Center is permitted access to the Internet through a firewall to obtain these updates, then a firewall change to open port 443 for the Security Center system will be required. Port 80 had been previously used and existing Security Customers will need to modify the firewall rule already in use for their Security Center system.

The following changes are included in Security Center 3.2.3:

Cumulative Vulnerability Data Base

- Tracking more logical date/time-stamp information regarding vulnerabilities that have been moved to the patched and mitigated database. Now, resolved vulnerabilities will show when the vulnerability was first discovered by Security Center and the date that it was resolved.
- Corrected several minor formatting and display issues with dynamically generated information.

Scanning

- The plugins list for the virus Check Scan policy has been updated.
- Several issues related to pausing scans and scheduled scans have been resolved.
- Better cleanup is performed when a scan policy is deleted.

Reporting Module

- NetBIOS names are now provided in the Vulnerable Systems Detail chapter of the Reporting module.
- All times zones are now available when defining a report.
- Several minor issues related to the display of certain data have been resolved.

Assets Module

- The process of updating dynamic asset lists based on new scan information is significantly faster than previous versions of Security Center.
- The assets-sample.xml file has been updated.
- Deleting multiple static asset lists at the same time may not have worked for all asset lists that were selected. This has been corrected.

Nessus Related

- Nessus v3.2 (currently in beta) will allow the addition of pre-compiled libraries. SC 3.2.3 provides support for uploading and use of the new .nlib files.
- Three Windows CIS compliance .audit files are now being provided with the Security Center base package.

Logging

- The log files for the version of Apache installed with Security Center are now periodically rotated and removed.
- Minor improvements to the Administrator log for readability and relevant information have been made.

SC Security & Auditing

- The plugins update processes for both Nessus and PVS have been modified to ensure that the connection used to retrieve the updates is secure, and that the packages are verified.
- PHP, OpenLDAP, and OpenSSL libraries/packages included with Security Center have been updated.
- The version of Apache included with Security Center has been updated.
- The SSL certificate included with Security Center has been updated.

- The ability to audit successful and failed login attempts is now provided.
- Entries are now made to the Administrator log when either successful or unsuccessful attempts to view the Administrator log are made.

General

- Several minor issues with filtering in the Cumulative Vulnerability DB, Analyze IDS Events, and Analyze Logs have been corrected.
- Corrected issues which arose in certain circumstances between Security Center and Thunder/LCE.
- Several improvements to error handling and error reporting.
- PVS plugins updates will no longer fail with PVS systems which are connected to Security Center over very low bandwidth connections.
- An issue in which the update for the Bleeding Snort rules could cause the update for the regular Snort rules to fail has been resolved.
- An issue which caused passively detected vulnerability data to delay appearing in the Patched and Missing database has been resolved.

Security Center 3.2.3 Hotfix01 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

As part of the release of Thunder 2.0.3 this Hotfix is being provided for those users of Security Center who also use Thunder.

The reason for this hotfix is that the showids binary and one of it's supporting files, TNS_ShowIDS.php, have been updated in Thunder 2.0.3 and must also be replaced in Security Center.

The showids binary is operating system specific and must be applied to a Security Center system running the correct OS. Please note that the Security Center services do NOT need to be stopped in order to install this hotfix. This procedure will have no impact on scans or other ongoing processes of Security Center.

The installation script will perform the following functions:

- Backup (copy) /opt/sc3/bin/showids
- Backup (copy) /opt/sc3/php-console/lib/TNS_ShowIDS.php
- Copy the new showids file into place
- Copy the new TNS_ShowIDS.php file into place
- Verify/set permissions on the new files

To install the files:

- Transfer the hotfix package to your Security Center system
- Extract the files to a temporary directory using the command:
  tar xvfz <Hotfix Package Name>
- A directory will be created under the extraction directory, change to this new directory
- Run the install.sh file that is in the directory

The old showids file will be copied to the following location:
/opt/sc3/bin/showids.backup.hotfix01

The old TNS_ShowIDS.php file will be copied to the following location:
/opt/sc3/php-console/lib/TNS_ShowIDS.php.backup.hotfix01

The new showids file will be copied to the following location:
/opt/sc3/bin/showids

The new TNS_ShowIDS.php file will be copied to the following location:
/opt/sc3/php-console/lib/TNS_ShowIDS.php

Security Center 3.2.4 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The significant changes in this version of Security Center provide security updates to third-party applications and libraries. Most notably are the recent updates to Apache and OpenSSL.

Changes in version 3.2.4 include:

- Update to SC Integrated Apache
- Update to OpenSSL

- Update to OpenLDAP
- Update to libxml2
- An issue found with a single-IP scan when no zone was selected in the scan configuration has been fixed.
- It is now possible to bind a recommendation to an SSH fingerprint.
- An issue has been resolved which would cause importing named static asset lists to fail.

Special Note when running Security Center on Red Hat Enterprise Server 3:

For those users of Red Hat Enterprise Server 3, after the upgrade to Security Center 3.2.4 you may experience a problem with the display of the text of tickets that are entered. The issue manifests when a single quote (') is used in the text of the ticket, in which an escape character (\) is added.

For Example: "This is the vulnerability that John\'s team was worried about."

Solution:

The file /opt/sc3/support/etc/php.ini does not get updated by the install process in order to protect any modifications that have been made. To correct this, edit the file and change the line that reads 'magic_quotes_gpc = On' to 'magic_quotes_gpc = Off'. Restart the HTTPD services ("service httpd restart") and the issue should be resolved.

Security Center 3.2.5 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Version 3.2.5 includes a couple of updates to third-party libraries/packages which have been released. These updates resolve security issues in support of our Common Criteria certification.

Changes in version 3.2.5 include:

- Update to Apache 2.0.63
- Update to PHP 5.2.5

Security Center 3.4.0 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

As they are significant, please refer to the following PDF file for the version 3.4.0 Release Notes:

Security Center 3.4.0 Release Notes

Security Center 3.4.1 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following details many of the changes that are included in version 3.4.1, the significant issues that have been resolved, as well as notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

General Notes

- As with any application, it is always wise to perform a backup of your Security Center installation before upgrading.
- A new default SSL certificate for Security Center is being provided in version 3.4.1 as the previous certificate expired on 5/22/08. This new certificate will be installed automatically. **If you have your own SSL certificate installed, be sure to back it up prior to upgrading, and restore it afterwards.**

Upgrading from 3.4.0

There are no special upgrade related notes. The command syntax for an RPM upgrade is as follows:

```
rpm -Uvh <RPM Package File Name>
```

Upgrading from Pre-3.4.0 Security Center Versions

- Please note that existing scan policies, as well as scheduled and template scan files will be modified as part of the update process. Please be sure to verify these files after the upgrade.
- After upgrading to Security Center 3.4 you may experience a problem with the display of the text of tickets that are entered. The issue manifests when a single quote (') is used in the text of the ticket, in which an escape character (\) is added.

  For Example: "This is the vulnerability that John\'s team was worried about."

  The file /opt/sc3/support/etc/php.ini does not get updated by the upgrade process in order to protect any modifications that you have made. To correct this, edit the file and change the line that reads "magic_quotes_gpc = On" to "magic_quotes_gpc = Off". Restart the HTTPD services (use the command "service httpd restart") and the issue should be resolved. New installations of Security Center will have this setting off by default.

- Security Center v3.4 is the first version in which the Red Hat ES5 operating system is supported. Those existing SC customers wishing to migrate their installations to ES5 must first upgrade their current installation of SC to v3.4, then follow the OS migration procedures as documented in the Cerberus knowledge base article titled "**Retaining Security Center 3 install when installing new OS**".

Application Notes

General

- A global change with regard to passwords has been made. At this time, all printing (non-control) characters of the ASCII character set are acceptable for passwords in all password fields within Security Center with the following exceptions:

Character	Description
<	Less than sign
>	Greater than sign
,	Comma
"	Quotation Mark (aka Double Quote)

- The new Firefox v3.0 browser has been tested with Security Center and all issues found have been resolved.
- The third-party library, libpng, has been upgraded to version 1.2.27. A security vulnerability had been discovered the previous version of the library and has been resolved in this version.
- The PHP scripting language which is used by Security Center has been upgraded to the latest version available, version 5.2.6.
- The third-party library, OpenSSL, used in Security Center was updated to version 0.9.8h, which is the latest version available. This library was updated to resolve discovered security issues.

Data Query Tools/Query Results Display

- An issue was resolved with the Time Direction Summary tool, in which it would return no results when used with the 'Type' filter.

Scanning/Scan Policies

- An issue has been resolved in which end-users of the Security Center system which have privileges for policy scanning were able to initiate individual plugins scans from certain portions of the interface.
- Previously, when selecting a scan policy in the Add Scan function, the policy identification numbers were not provided along with the policy names.
- An issue has been resolved in which dependent scans would run properly the first time they were triggered, but would fail to run afterwards.
- An issue has been resolved which would cause a scan initiated using SSH local checks to produce errors on the Additional Information page of scan management.
- An issue has been resolved with scanning in which using an asset list which is configured with SMB credentials would not run.

Administration

- Deleting user accounts which used LDAP authentication would previously not result in complete removal of the account.
- A modification has been made to the logging of PVS plugin updates so that they are less verbose by default. This has been done to make the admin log more usable.
- Several role related permissions issues have been resolved for both manager and end-user account types.
- There was previously an error generated, only when running Security Center on Red Hat ES5, when adding a Nessus scanner and selecting "Authenticate with an SSL certificate".
- Customers using many asset lists and long names for each list will no longer experience problems when assigning large numbers of asset lists to users. This problem was noted when using Microsoft Internet Explorer, but it was possible to see it in other browsers.
- An issue has been resolved in which very long passwords were not being accepted for login, essentially locking out the account.

Reporting

- Issues in certain XML report templates which would result in error messages when running the report have been resolved.
- The Service Detection report chapter would not show the ports on which a service was found.

Nessus Related

- Several issues related to uploading .nessus files have been resolved.
- The facility has been added for downloading a .nessus file from scan data which has been manually imported to the Security Center.

IDS & LCE/Thunder Related

- An issue in Analyze Logs prevented the viewing of Raw Syslog events beyond the first twenty-five.

IDS Related

- A problem has been resolve that caused Snort IDS signature updates to fail without notification.

Security Center 3.4.2 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Changes in version 3.4.2 include:

- Extended the possible number of extended plugins to over 5000.
- Fixed an issue which limited Scan Policies to 87. Limit is now 500.
- Fixed multiple issues dealing with credentialed scans.
- Fixed an issue on the disable checks page where .select all. and .unselect all. buttons were not working correctly.
- Fixed an issue in which users with long usernames would initially show no vulnerabilities.
- Fixed an issue in which when a user is deleted, old reports belonging to that user were left behind. They are now deleted as well.
- Updated the default Report Logo.

- Fixed an issue in which LDAP user info might be incorrectly overwritten when attempting to refresh from the LDAP server.

Security Center 3.4.2.1 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Version 3.4.2.1 of Security Center is a security update:

- Two security issues involving access to system files by authenticated Security Center users have been resolved. Users who had successfully logged into Security Center with valid credentials could obtain system files.
- Recent security updates to the following 3rd-party dependencies have been included:
  - Apache (v2.2.9)
  - libmcrypt (v2.5.8)
  - libpng (v1.2.32)
  - libxml2 (v2.7.2)
  - OpenLDAP (v2.4.11)
  - OpenSSL (v0.9.8i)
  - SQLite (v3.6.3)

Tenable recommends that all Security Center customers upgrade to version 3.4.2.1.

Security Center 3.4.3 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Note: A recorded webinar by Tenable founder, Ron Gula on the Security Center 3.4.3 features is available.

The following list describes many of the changes that are included in Security Center version 3.4.3, the significant issues that have been resolved as well as notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

General Notes

As with any application, it is always wise to perform a backup of your Security Center installation before upgrading.

Upgrading from 3.4.0

There are no special upgrade related notes. The command syntax for an RPM upgrade is as follows:

```
rpm -Uvh <RPM Package File Name>
```

Compatibility with other Tenable software

There are a number of new features in SC 3.4.3, LCE 3.0.1 and the LCE 3.x clients that are only available if all three products are running the software versions that support the new features. The products will function together if they are not all upgraded, but some of the new features may not be available.

Upgrading from Pre-3.4.0 Security Center Versions

- Please note that existing scan policies, as well as scheduled and template scan files will be modified as part of the update process. Please be sure to verify these files after the upgrade.
- After upgrading to Security Center 3.4.x you may experience a problem with the display of the text of tickets that are entered. The issue manifests when a single quote (') is used in the text of the ticket, in which an escape character (\) is added.

  For Example: "This is the vulnerability that John\'s team was worried about."

  The file /opt/sc3/support/etc/php.ini does not get updated by the upgrade process in order to protect any modifications that you have made. To correct this, edit the file and change the line that reads "magic_quotes_gpc = On" to "magic_quotes_gpc = Off". Restart the HTTPD services (use the command "service httpd restart") and the issue should be resolved. New installations of Security Center will have this setting off by default.
- Security Center v3.4 is the first version in which the Red Hat ES 5 operating system is supported. Existing SC customers wishing to migrate their installations to ES 5 must first upgrade their current installation of SC to v3.4.x, then follow the OS migration procedures as documented in the Cerberus knowledge base article titled "**Retaining Security Center 3 install when installing new OS**".
- All release notes for Security Center versions 3.4.0 and later are applicable and should be reviewed. These release notes may be found on the **Tenable Customer Support Portal**, in the

Downloads section, under the Security Center portion of the **Security Center, 3D Tool and xTool** page.

Application Notes

General

- Minor improvements for ease of use and intuitiveness have been made throughout the GUI.
- The PHP scripting language that is used by Security Center has been upgraded to the latest version available, version 5.2.8.
- The following 3rd-party dependencies which are used in Security Center have published updates which have been included in version 3.4.3:
  - libpng has been upgraded to version 1.2.34
  - libxml2 has been upgraded to version 2.7.2
  - OpenSSL has been upgraded to version 0.9.8j
  - SQLite has been upgraded to version 3.6.7
  - Apache has been upgraded to version 2.2.11

LCE Related

- A single Security Center customer can now connect to, receive alerts and query data from multiple LCE systems.
- The new functionality in LCE that allows user names to be associated with events has been enabled in this version of Security Center.
- Security Center is now able to access the new Raw SYSLOG Search feature of LCE 3.0.
- Functionality has been added to permit a query of an archived LCE data silo. Archival of these silos was recently introduced in LCE v3.0.

LCE & IDS Related

- Functionality has been added in which email alerts can be generated for any specific event provided to the Security Center by an IDS or the Log Correlation Engine, regardless if they correlate with a vulnerability or not.

- Graphs for users, events and types when viewing log data have several improvements for readability including time scales that correspond to the active query.
- The ability to view LCE archive data has been added. This feature only applies to LCE server at version 3.0 or higher.

IDS Related

- Support for the updated NetScreen/IDP SYSLOG event formats has been added.
- Support for the updated TippingPoint SMS IDS alert format has been added.

Data Query Tools/Query Results Display

- End-users are able to open tickets with comments or recommendations from any of the Vulnerability analysis pages.
- When viewing information using any analysis screen's Sum by IP tool, clicking on an IP address will pop-up an information window that includes the following sections:
    - System Info: Displays information about the OS, NetBIOS, DNS Name (if known), MAC address, Last Scan as well as the availability of Passive and Compliance data.
    - Assets: Displays which Security Center asset lists the IP address belongs to.
    - Vulnerabilities: Displays a bar chart summary of vulnerabilities for this IP.
    - Resources: Provides URLs for obtaining further information. It is also possible to add custom links to this section.
- Significant improvements to the query management system have been made.
- Minor ease of use modifications have been made to filtering when using the analysis tools.

Nessus Related

- Support has been added for the three new Nessus PCI DSS compliance plugins:
    - 33929 PCI DSS compliance
    - 33930 PCI DSS compliance: passed
    - 33931 PCI DSS compliance: tests requirements

- Support has been added for the new Nessus feature that limits attempts to login to scan targets so that only the credentials provided in the scan policy, and no generic accounts, will be used.
- The sorting and searching of plugins has been improved for ease of use.

Scanning/Scan Policies

- Credentialed scans on Unix/Linux target hosts now have the ability to elevate privileges via su/sudo.
- The NetStat port scanner is now integrated into the Add Scan and Scan Policy Options screens as a port scan option and may be used in addition to, or in place of, the TCP Full and TCP SYN port scans.
- The plugins selection (enabling and disabling plugins) for scan policies has been modified for ease of use and consistency.
- Configuring scans with SSH keys that include a passphrase now works properly.
- It is now possible to enter long strings of port ranges when configuring a scan or scan policy.
- Manually launching a recurring scheduled scan, then deleting it, no longer causes the *vpolicy* file to delete.
- Setting the Disable Host Ping option now works properly.

Administration

- The Nessus Scanner Management administrator option has been redesigned for ease of use and to remove the 10 zones and 16 scanners per zone limitations. You may now add up to 100 scanners, 100 zones and 500 network ranges from the Security Center management interface.
- The Log Correlation Management administrator option has been redesigned for ease of use and provides new features in support of multiple Log Correlation Engines.
- The "**LCE Status Message Legend**" button displays an information box containing possible returned status messages from LCE and a brief description of these messages.
- All default settings for options in the "**Configure the Security Center**" menu are now displayed.
- The Security Center status may now be determined from the command line on the SC server with the following command:
  # service SecurityCenter status

- A new configuration option has been added to allow Security Center administrators to define the interval in which SC resynchronizes with its Nessus scanners. This is most relevant to large SC installations with many Nessus scanners from which very frequent or constant scanning is performed.
- Facility for SC administrators to "Reset" the Nessus plugins activation code has been added for ease of code replacement and troubleshooting connectivity issues.
- A new tab labeled "Customization" is now displayed for the admin user and provides the following selections:
  - Security Center Logo Management
  - Security Center Reports Logo Management
  - Manage "IP Address Information" Links
- The "Manage IP Address Information" selection provides the ability to add dynamic URLs to the list of resource links displayed in the "Sum by IP" Analysis Tool.

Reporting

- The functionality for the addition of a custom report logo has been modified so that they can now fit in the bottom of the page, to an effective max size of 500x175.
- Report generation process logging has been enhanced.
- An issue which prevented certain user accounts from downloading reports has been resolved.

Security Center User Accounts

- A period (.) is now a permitted character in both Security Center user account names, as well as asset list names.
- It is now possible to create a security manager user account with no scanning privileges.

Security Center 3.4.3 Hotfix02 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The reason for this hotfix is that an issue has surfaced with the display of LCE data after Daylight Savings Time begins. This issue does not affect Security Center or LCE data or configuration files in any way. This issue is related to the introduction of time 'tick' marks into the graphs and only affects the display of certain graphs in Security Center.

The graphs that are affected are those that inlcude the DST changeover date/time and also were created with a date range of less than 10 days.

This hotfix is for those users running Security Center 3.4.3 and is OS independent.

Security Center 3.0.3 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

New Features in 3.0.3

- Better data validation on static asset list uploads
- Enhanced asset list management features
- Increased performance for cumulative database "All Assets" queries
- Resolved an issue with URLs not being displayed
- Addressed an issue with remediation scans
- Ticketing email issue resolved

Security Center 3.4.4 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Watch the SC 3.4.4 and LCE 3.2 Webinar with Tenable founder, Ron Gula, including demonstrations of the new LCE 3.2 full log search functions.

The following list describes many of the changes that are included in Security Center version 3.4.4, the significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

General Notes

As with any application, it is always advisable to perform a backup of your Security Center installation before upgrading.

Upgrading from 3.4.x

There are no special upgrade notes for those users running Security Center 3.4.0 or later. The command syntax for an RPM upgrade is as follows:

```
    # rpm -Uvh <RPM Package File Name>
```

Compatibility with other Tenable Software

There are a number of new features in Security Center 3.4.4 and Log Correlation Engine (LCE) 3.2 that are only available if both products are running the software versions that support the new features. The products will function together if they are not all upgraded; however, the new features will not function.

Upgrading from Pre-3.4.0 Security Center Versions

- Please note that existing scan policies, as well as scheduled and template scan files will be modified as part of the update process. Please be sure to review these scan files after the upgrade and ensure that the PARENT_POLICY keyword is present.
- Security Center version 3.4 is the first version to support Red Hat ES 5. Existing Security Center customers wishing to migrate their installations to ES 5 must first upgrade their current installation of Security Center to version 3.4, then follow the OS migration procedures as documented in the Customer Support Portal knowledge base article titled "**Retaining Security Center 3 install when installing new OS**".
- It is recommended that all release notes for Security Center versions 3.4.0 and later be reviewed prior to upgrade. These release notes may be found on the **Tenable Customer Support Portal** in the **Downloads** section under the Security Center portion of the **Security Center 3D Tool and xTool** page.

Application Notes

General

- FIPS 140 support has been compiled into the OpenSSL that is used by Security Center for secure socket layer connections.
- The "mod_rewrite" functionality has been compiled into Apache as used by Security Center to enable users to configure their systems for completely encrypted browsing. Enable these settings by adding the following lines at the bottom of /opt/sc3/support/conf/httpd.conf and then restarting the Security Center web service:

```
# mod_rewrite rules to convert URLs to use SSL
RewriteEngine On
RewriteMap lowercase int:tolower
RewriteRule ^/(.*)$ https://${lowercase:%{SERVER_NAME}}/$1
```

For more information regarding "mod_rewrite" refer to the Apache documentation.

- Security Center web server wget responses no longer include PHP or Web Server version information.

Data Query Tools/Query Results Display

- The maximum number of log events viewable under "Analyze Logs" has been raised by increasing the number of digits allowed in the Output Filter input box of the Log Analysis screen from eight to ten. Input is further checked to ensure the results will display no more than 4,294,967,295 events - the maximum number of events the system is capable of displaying. Previously, the maximum number of viewable events was 9,999,999.
- For FDCC requirements, all CVSS2 scores in the "full vuln detail" screen now have a URL that takes the score and populates a query to NIST for CVSS2 analysis.

LCE Server Related

- Users now have the option under "Events" -> "Search Raw Logs" to view historical LCE data across multiple LCEs. Because of the potential for large amounts of LCE data, raw logs are stored compressed on the LCE servers and on the Security Center. This feature requires configuring two options in /opt/lce/daemons/lce.conf: "enable-log-archiving" and "archive-directory". Data collected through "enable-log-archiving" is stored in the directory specified by "archive-directory".
- The LCE log archive module maintains usage statistics that are available through the console under "Events" -> "LCE Archive Status" for users who have enabled "enable-log-archiving" for compressed raw log storage.
- User access is configurable on a "per-LCE" basis for raw log data stored using the "enable-log-archiving" function. Configure this option through "Users" -> "Manage LCE Access".

Nessus Related

- Support for the Nessus Enable "CGI scanning" setting option is now available within the Security Center scan "Options".

- Support for Database compliance checks is now available through Security Center scan "Options". Enable this option on the "Add New Scan" page through the checkbox "Perform Database Analysis" that enables or disables the database compliance check plugins. The supporting options are Username and Password, System ID, and database type. Available database scan targets include:
    - Oracle
    - Microsoft SQL Server
    - MySQL
    - PostgreSQL
    - DB2
    - Informix

  More information on Database Compliance checks is available within the Nessus Compliance Checks documentation.

Scanning/Scan Policies

- The contents of an audit file stored on the Security Center console are now viewable by double clicking on the file name within the scan "Compliance" window.
- There is a new scan preference within the scan "Options" named "Start the Registry Service During a scan". This option temporarily enables the "Remote Registry" service on the scanned Windows systems to allow for more complete system scans.
- If SSH keys are used for scan authentication, a "reset" button is now available to enable the addition of new SSH keys as needed.
- Compliance policy files may now be deselected using the "Un-select audit files" command button available within the scan "Compliance" section.
- When configuring SMB passwords, second and third passwords are now used. Previously there was an issue where a scan login would fail if the first SMB password field was left blank, but the second or third SMB password fields contained valid logins.

IDS Related

- Support for the Sourcefire IMS IDS alert format has been added. The Sourcefire alert source must be configured as "Snort" for the alert input to be parsed properly.

Administration

- A new option, "Remove old email archives after", is now available for the admin user under "Console" -> "Configure the Security Center" -> "Email Delivery Options". This option is configured by default to one month and is used to remove old sent emails from the Security Center. Previously these emails would build up indefinitely.

Reporting

- Report Templates now use a new timeframe option "7d" that allows LCE/IDS queries to go back seven days from the current date. Previously, this timeframe option was not available causing report template options to be incorrectly overridden by LCE filter options.

Security Center 3.4.5 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Watch the Security Center 3.4.5 Release Video by Tenable CTO, Ron Gula.

The following list describes many of the changes that are included in Security Center version 3.4.5, the significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Important

Starting with Security Center 3.4.5, if Security Center exceeds its license key IP limit, only administrator logins are allowed with limited functionality. An opportunity is given to upload a new license key to accommodate the excess IP count and restore functionality. Contact support@tenablesecurity.com to obtain a new license key if necessary.

General Notes

As with any application, it is always advisable to perform a backup of your Security Center installation before upgrading.

Upgrading from 3.4.x

There are no special upgrade notes for those users running Security Center 3.4.0 or later. The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh <RPM Package File Name>
```

Application Notes

General

Bundled third-party products updated include newer versions of: Apache, libpng, PHP and SQLite.

Scanning/Nessus Related

Support has been added for the enhanced web application testing settings introduced with recent Nessus plugin modifications. It is important to understand the following requirements for web application test scans:

- Only one web server can be scanned per web application test.
- Scanned hosts must be specified within the Security Center scan page in the following format: [IP:domain_name] or [IP:hostname]. An example of a scanned system would be:
  192.0.2.150:www.example.com
  Or:
  192.0.2.150:mywebhost

New Scan options:

Web Application Test Settings:

- Enable Web Application Tests
- Send POST Requests
- HTTP Parameter Pollution
- Test embedded web servers
- Maximum Run Time (min)
- Combos of arguments values
- Stop at first flaw

More information can be found at: http://blog.tenablesecurity.com/2009/06/enhanced-web-application-attacks-added-to-nessus.html.

Reporting

The following new reporting templates have been added:

- Windows Patch Summary Per Host.xml - filters on plugin 38153 for a concise list of hosts that have missing SMB patches and which patches are missing.
- Scanned Hosts in Last 90 Days.xml - lists all hosts with a completed scan in the last 90 days
- Scanned Hosts in Last 30 Days.xml - lists all hosts with a completed scan in the last 30 days
- Scanned Hosts in Last 7 Days.xml - lists all hosts with a completed scan in the last 7 days
- CCE Configuration Summary.xml - Summary of all Nessus compliance checks that contain "CCE" in their name. This report will summarize the compliant and non-compliant hosts with respect to the FDCC and other SCAP style audits.
- CCE Configuration Report.xml - Report of all Nessus compliance checks, tested hosts, tested Windows servers and raw test results that contain "CCE" in their name. This report will detail the compliant and non-compliant hosts with respect to the FDCC and other SCAP style audits.
- PCI Configuration Summary.xml - Summary of all Nessus compliance checks that contain "PCI" in their name. This report will summarize the compliant and non-compliant hosts with respect to the PCI audit policies maintained by Tenable.
- PCI Configuration Report.xml - Report of all Nessus compliance checks, tested hosts, tested Windows servers and raw test results that contain "PCI" in their name. This report will detail the compliant and non-compliant hosts with respect to the PCI audit polices maintained by Tenable.

Misc/Enhancements

- Scan results import process improved - The cumulative database (HDB) will no longer be converted to .nessus during scan imports. The HDB conversion will occur as part of the nightly processes.
- SSH/LCE connection reduction - performance improvement
- Change default refresh time for Nessus from one to 12 hours
- Increased the email size limit to 16MB
- Security Center is now officially supported on CentOS 5
- First seen and last seen dates being shown for scan and new scan results (requires browser cache to be cleared after upgrade)

- Delete Static Assets menu item's name has changed to Static Asset List Add/Edit/Delete (See New Screen)
- Plugin IDs report filter (now accepts up to 16 plugin IDs vs. four)
- PSM should be able to edit contents of a static asset range
- Choosing an Asset List & an adhoc IP causes scan to fail
- Sourcefire modified download process of Snort rules requiring change to snort_update.pl (version 2.8 Snort ruleset support).
- Option to enable/disable Build splash screen from Admin login
- Total Active IP count now correctly includes hosts scanned for compliance checks.
- Policy plugin load page speed and stability improved.

Security Center 3.4.6 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in Security Center version 3.4.6 and the significant issues that have been resolved. A PDF file of these release notes is also available here.

Enhancements

Snort IDS Signature Updates

Enabling "Nightly update of Snort signatures" now pulls the snort.ids.gz file from Tenable's web site (and not from Sourcefire (http://www.snort.org) or Emerging Threats.net (http://www.emergingthreats.net)). Tenable downloads the signatures and produces an aggregated snort.ids.gz file that is downloaded by the Security Center. Once downloaded, a snort.ids file is placed in the /opt/sc3/admin/ids directory.

The following options have been removed from the "Console -> Configure the Security Center" page:

- Oinkmaster Snort HASH
- Download Emerging Threats Snort signatures

Event Alerting

Customers must have an IDS source configured to manage event alerts. An error message is displayed when navigating to the Event Alerting page if no IDS source has been configured.

List OS Analysis Tool

The "List OS" page for passive data now includes the type of device, if detected. Otherwise, "general-purpose" is displayed. This differs for active data where only the OS type is displayed.

Scanning/Licensing

Plugin 12053 (FQDN of the remote host) no longer counts towards the IP license.

Third Party

Upgraded the following third-party dependencies to the specified versions: OpenLDAP 2.4.21, OpenSSL 0.9.8o, Apache 2.2.15, PHP 5.2.14, SQLite 3.6.23.1, libxml 2.7.7, libpng 1.2.44.

Bug Fixes

This is a rollup release and includes all fixes previously provided for Security Center 3.4.5 in hotfix01-hotfix04.

Hotfix01 for Security Center 3.4.5 (11/2/2009)

Static Asset List Add/Edit/Delete Screen:

This hotfix addresses several issues discovered with the "Static Asset List Add/Edit/Delete" screen:

- The Entries column previously reported the incorrect number of entries an asset list contained
- Adding multiple IPs/CIDRs/Ranges to an asset list incorrectly displayed an error
- The ability to delete the "Customer Ranges" static asset list has been added
- An error was incorrectly displayed when attempting to edit an asset list, that prevented the asset list from being edited

Hotfix02 for Security Center 3.4.5 (12/14/2009)

IDS Splash Screen: The "Top 10 Vulnerabilities-Security Event Analysis for last 7 days" chart does not display for asset lists with a file name that contains a space. By design, Security Center will update the splash charts when the next nightly updates occur. As of SC 3.4.5, the splash screen generation is optional but enabled by default. This option is evident for Security Center administrators, under the "Console -> Configure the Security Center" page, as "Enable splash screen chart updates". If this option is turned off, then the last generated splash chart will be displayed.

CSV Exports for Vulnerability Data: Large CSV exports for vulnerability data were truncated (in certain cases) to 10,000 lines. For example, if you request a CSV using the "Display Vuln Details" analysis tool and the total number of vulnerabilities is 27,000, you would only get a CSV consisting of 10,000 lines, instead of 27,000.

IDS Correlation: IDS correlation was not functioning as expected in 3.4.5. When navigating to "Events -> Analyze IDS Events" in the Security Center GUI and applying the Correlation Filter (by selecting "Yes" from the drop down menu), if there were events that correlated to vulnerabilities, a "No Records Found" message was always displayed.

Patched & Mitigated - First Observed/Last Discovered: First Observed and Last Discovered fields (in most cases) displayed the current date instead of the date of the event. This issued may have occurred if using Tenable's Passive Vulnerability Scanner (PVS) or you had imported scan data manually using the import_manual.pl script.

Comments Converted into Garbage When Opening Tickets: In some cases when tickets were entered for vulnerabilities, the comment text was converted to garbage because of an issue with MSIE6 and browser caching. Tenable recommends clearing your browser cache after applying this hotfix.

Plugin Output for Nessus "os_fingerprint.nasl" Plugin: A minor issue with the handling of the os_fingerprint.nasl plugin output has been corrected.

Plugin Updates Fail: In certain cases, plugin updates fail for Nessus scanners when using a proxy.

Hotfix03 for Security Center 3.4.5 (1/8/2010)

Scans Scheduled for 2010 Display "Launch Window Exceeded": Scans scheduled for the year 2010 would display "launch window exceeded" as their status message when the scan was submitted. However, the scan ran for the date/time that it was scheduled for, even though Security Center indicates otherwise.

Cannot Download .nessus Files from "Browse Individual Scan Results" Screen for 2010: An issue has been addressed that prevented downloading .nessus files from the "Browse Individual Scan Results" screen for a scan that completed in the year 2010. When trying to download the .nessus file, a screen was displayed with the text "Bad Date".

Large IDS Files Cause logd to Crash: The logd daemon would crash when it attempted to access a file larger than 2GB.

Hotfix04 for Security Center 3.4.5 (3/17/2010)

Certain Combinations of Asset Ranges Causes Scan to Fail: An issue was corrected where scans would fail to launch when using certain combinations of asset list ranges.

Randomize Target IPS - Scan Option: This option is no longer valid and has been disabled.

Scans Fail Using an Uploaded Static Asset List That Contains Spaces/Newline Chars: An issue has been addressed for scans failing to launch when using an uploaded static asset list that contains spaces and/or newline characters.

Rollover Scans Renamed Incorrectly: An issue has been addressed where rollover scan file names were being renamed incorrectly. This issue would prevent the Manage Scan options in the SC3 GUI from functioning properly.

SecurityCenter 4.0 Upgrade Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes the known issues with upgrading to SecurityCenter 4.0 from Security Center 3.4.x. A PDF file of these release notes is also available here

For detailed upgrade instructions, please reference the SecurityCenter 4.0 Upgrade Guide.

Scanning/Nessus Related

1. Some Scan Policy parameters may not be set correctly after upgrading from Security Center 3. These settings did not appear as configurable options in Security Center 3 policies, so when those policies are brought over to SecurityCenter 4, the settings will have to be changed to "unlimited", the default value when adding a new policy in SC4.

    - Change "Max Scan Time (hours)" from "2" to "unlimited"
    - Change "Max TCP Connections" from "1" to "unlimited"
    - Change "Silent Dependencies" from "unchecked" to "enabled"
    - Port Scan settings may need to be re-entered

2. By default, Organizational users, other than Organization Head users, are not granted access to the Repository or any pre-defined assets for the customer they were migrated from. Users may not be able to view vulnerabilities or scans post-upgrade. Edit the user, select the "Access" tab and ensure that the desired Repositories and Assets are associated.

Notifications

The upgrade process removes the SMTP Port and Return Address. These settings must be re-entered from the "Admin" GUI after the migration process has completed.

LCE Related

Note: SecurityCenter 4 requires LCE servers to be upgraded to 3.4.1 for interoperability. After upgrading from Security Center 3.4.x to SecurityCenter 4.0, users are unable to view Events from pre-existing LCEs. This is caused by the known_hosts file not being copied over from "/opt/sc3/.ssh/" to "/opt/sc4/.ssh/" during the upgrade. If the file is manually copied, users are then able to view events for those pre-existing LCEs.

IDS Related

IDS Correlation has moved from SecurityCenter to the LCE. Refer to the SecurityCenter 4.0 Architecture document for more information.

Miscellaneous

The following items are not migrated during the upgrade. Items that can be recreated must be done so post-upgrade:

- Custom reports
- Nessus scans
- Individual scan results
- Vulnerability trend snapshots
- Raw log searches
- Audit files
- IDS events (new IDS events will be stored on the LCE)

SecurityCenter 4.0.1 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in SecurityCenter version 4.0.1, the significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here

Upgrade Notes

In 4.0.1, we now handle the following items during the upgrade:

- Import Scans (Schedules) from SC3 - The upgrade wizard will import scans (both recurring and templates) and attached policies and assets. Credentials will still need to be re-associated to any scans that require them.
- Audit files are now copied over from SC3 and added as Application audit files.
- Fixed the assignment of repository and assets that were imported from a customer during migration. They are no longer added as organizational assets and are now added as user objects and shared to all users as defined and filterable assets. (In SecurityCenter 4.0, this affected any users other than the org head.)
- Nessus certificates are now copied over during migration.
- Individual Scan Results - A script is provided to import individual scan results (after import, results can be viewed from the "scan Results" page; they will not be re-imported into the cumulative database).
- Vulnerability Trend Snapshots - A script is provided to import historical snapshots from an SC3 customer into a SecurityCenter 4 repository to retain vulnerability trend information.
- Fixed an issue following an upgrade from SC3 where migrated LCEs initially had a status of "Invalid Certificate" that caused the inability to view events for pre-existing LCEs. The upgrade wizard now includes the known_hosts file during the copy of the RSA/DSA SSH keys.
- If a custom SSL certificate is encountered, it will be preserved during the upgrade process; otherwise a new certificate will be dynamically generated.

* Other items that are not migrated include custom reports, one-time and dependent Nessus scans, raw log searches and IDS events.

After completion of the upgrade process from SC3 to SecurityCenter 4, be sure to allow a period of time for the upgrade process to complete the migration. Even though the wizard indicates the upgrade is complete, navigating the console may result in a server time-out.

Importing Vulnerability Trend Snapshots from SC3

Usage:

```
# convertSnapshots.php [Customer ID][Repository ID][Days]
```

Arguments:

- [Customer ID] - A valid customer serial number from SC3
- [Repository ID] - A valid repository ID from SecurityCenter 4
- [Days] - Number of days from the current date to pull snapshots from SC3

Example:

```
# /opt/sc4/support/bin/php /opt/sc4/src/tools/convertSnapshots.php 10 1 30
```

Run the command without any arguments to obtain a list of existing repositories and customer IDs on the system.

Example:

```
# /opt/sc4/support/bin/php ./convertSnapshots.php
Usage:  ./convertSnapshots.php [Customer ID] [Repository ID] [Days]
        [Customer ID]   - A valid customer serial number from SC3
        [Repository ID] - A valid repository ID from SC4
        [Days]          - Number of days back from the current date to
pull snapshots from SC3
        Example: ./convertSnapshots.php 10 1 30

Available Repositories:
        Repository Target1_ClassC's ID is 1
        Repository Target2_ClassC's ID is 2
        Repository Entire_Range's ID is 3
```

Importing Individual Scan Results from SC3

Usage:

```
# convertIndiScans.php [Customer ID][Organization ID][Days]
```

Arguments:

- [Customer ID] - A valid customer serial number from SC3
- [Organization ID] - A valid organization ID from SecurityCenter 4
- [Days] - Number of days from the current date to pull individual scans from SC3

Example:

```
# /opt/sc4/support/bin/php /opt/sc4/src/tools/convertIndiScans.php 10 1 30
```

Run the command without any arguments to obtain a list of existing customers and organization IDs on the system.

Example:

```
# /opt/sc4/support/bin/php ./convertIndiScans.php
Usage:  ./convertIndiScans.php [Customer ID] [Organization ID] [Days]
        [Customer ID]     - A valid customer serial number from SC3
        [Organization ID] - A valid organization ID from SC4
        [Days]            - Number of days back from the current date to
pull individual scans from SC3
        Example: ./convertIndiScans.php 10 1 30

Available Organizations:
        Organization Content's ID is 1
        Organization Test's ID is 2
```

The data migration tools are located in /opt/sc4/src/tools. You must have an existing SC3 installation on the same machine where you are executing the migration tools. The SecurityCenter services must be stopped before running this tool. If upgrading to 4.0.1 from 4.0 the scripts can still be used as long as the /opt/sc3 directory is still available on the system. Only run these scripts once. If a user runs these scripts more than once, the data does not overwrite and it will continue to add or duplicate data.

Changes and New Features

- A native 64-bit build is now available for ES 5 platforms.
- Scanning
  - Added support for su+sudo SSH credentials. Nessus recently added the ability to support su+sudo that allows a user to authenticate as user "user1" and then become user "user2" instead of user "root".
  - Added support for Cisco Compliance Checks as well as the required Cisco "Enable" privilege escalation attribute for SSH Credentials.
  - Plugin ID 10180 (Ping) is now ignored as far as license counts.
- Accept/Recast Risk
  - Added two permissions to roles that will enable/disable the "Accept Risk" and "Recast Risk" functionality. Updated the default Manager role to have both permissions enabled and the default End User role to have them both disabled by default.
  - Added a details button on the admin screens for managing accept/recast risk rules. The details show who created it, what organization they are in and the ticket comments.
- Alerts
  - An "Evaluate" button has been added to the alert module. The option allows an alert to be tested immediately whether or not it has met the configured time interval. This is useful for verifying new alerts after creation.
- Reporting
  - Improved word-wrap feature for long plugin names with no spaces.
- Vulnerability Analysis
  - New vulnerability list drill down to detail of IP/vuln.
  - In the "Detailed Vulnerability List" tool, the "Host Detail" Summary is now displayed when clicking on the IP address located in the vulnerability header.
  - A sort indication arrow is now displayed for the IP Address/DNS Name/MAC Address/NetBIOS Name column header in the "IP Summary Tool".

- Job Scheduling
  - Previously, if the job scheduler (Jobd) was down for an extended period, all of the jobs that would have run were kicked off immediately upon restart. This has been changed so that missed jobs are cleared and schedules re-added on service restart.
- Admin Dashboard
  - The LCE Overview dashboard now displays up to 1,000 LCE clients in a scrollable component, previously only 10 LCE clients were shown.
- Configuration
  - When editing Repositories or Organizations, you can now reset Repository Access to all users within an Organization or restrict access to just the Organization Head.
  - Adjusted the default End-User role permissions - removed full scanning, policy creation and accept/recast risk permissions.
  - The 1024 character limitation has been removed for "IP Ranges" when adding/editing new scans, scan zones or repositories, as well as "Restricted Scan Ranges" in organizations.
  - The size of a repository's raw DB file (hdb.raw) is limited to 4 GB. If an import of vulnerability data is attempted that would exceed this limit, the import will fail with a log message indicating that the max size has been reached.
- Online Help
  - Contextual Help has been added, clicking on the help link in the SecurityCenter 4 console will take you to the appropriate help page associated with the module you are currently viewing.

Fixes Previously Released for SecurityCenter 4.0.0 as Hotfix 01

SC 4.0.1 includes all fixes that were addressed as part of SecurityCenter 4.0.0 Hotfix 01, including the following:

- Upgrade Related Error Messages
  - Addresses several issues that caused an "Unable to initialize upgrade wizard" error message. This error is followed by one or more additional messages including:

        - Unable to prepare users.
        - Unable to retrieve user details.
        - Unable to parse workflow configuration.
        - Unable to parse the Lightning-Proxy configuration file. The file is malformed.
    - The "Next" button is not enabled in the upgrade wizard when there is invalid data in a severity filter or a missing operand in pluginID query filter.
- Compliance Scans
    - Corrects an issue in environments that had compliance data prior to the upgrade and were unable to run compliance scans afterwards.
- Web Proxy
    - Plugin updates were not utilizing the proxy settings. The format for the web proxy host settings is now the same as it was for SC3.
 http://[ip]:[port]/ or https://[ip]:[port]/
- Scan Policies
    - Attempting to change a new scan policy from user visibility to organizational visibility fails when the scan policy has an audit file attached to it.
- LDAP Validation
    - LDAP validation prevented an organization's head user from using a blank password.
- Scanning with Audit Files
    - When scanning with an audit, the wrong organization ID was sent to the scanner.
- License Issue
    - An issue has been fixed where certain licenses would fail to work properly.

SecurityCenter 4.0.2 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in SecurityCenter version 4.0.2, the significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrading from 4.0.x, there are no special upgrade notes for those users running SecurityCenter 4.0.0 or later. The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

If upgrading from 3.4.x, reference the Upgrade Guide on the Tenable Support Portal: http://cgi.tenablesecurity.com/SecurityCenter_4.0_Upgrade.pdf

Changes and New Features

- Scanning
  - Users now have visibility of their subordinate's scan schedules. They are also able to pause, resume and stop the scans of users beneath them. Both an "Owner" column and an "Owner" filter have been added.
  - Added the ability to copy Scan Schedules.
  - Added support for specifying the time zone in a scan schedule.
  - The import process has been changed to no longer import the results of a scan if the license will be exceeded as a result. An additional "Import" button has been added to the button bar of the Scan Results page. This button will be enabled for successful scans, and scans that were run successfully but failed on import.
- Analysis
  - Vulnerability query performance improvements.
  - Added a drill-down to the "Host Detail" screen from event IP summary. This is similar to the screen available when clicking on an IP address in the vulnerability IP Summary screen.
  - Added additional hyperlinks for external references to CVE, BID and OSVDB in the full vulnerability detail output.
- Support Watchlists

- Reporting
  - Added two new "hybrid" vulnerability detail report types; the report will summarize all hosts affected by a particular vulnerability. There are two variations of the report: One with a simple list of IPs per vulnerability, the other with detailed host information such as DNS, NetBIOS, and MAC. The new tools are listed as additional analysis tools available when adding a "table element" in reporting:
    - Vulnerability Summary - IP Detail
    - Vulnerability Summary - IP List
  - New HIPAA reports - There are six new Health Insurance Portability and Accountability Act (HIPAA) report templates that can be loaded when creating a report definition.
  - Added the ability to copy report definitions.
  - Users now have visibility of their subordinate's report definitions. Actions available on reports owned by users beneath them include Details, Pause, Resume and Stop.
- Exporting Data
  - Support for full .nessus v1 system tags available during export. The following tags were not previously populated correctly:
    - <netbios_name>Unknown</netbios_name>
    - <mac_addr>Unknown</mac_addr>
    - <dns_name>Unknown</dns_name>
    - <os_name>Unknown</os_name>
  - Scan settings are now included in the downloaded .nessus file. Previously, only the results were exported.
- Ticketing
  - Email notification sent on ticket creation

SecurityCenter 4.0.3 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in SecurityCenter 4.0.3, the significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

There are no special upgrade notes for those users running SecurityCenter 4.0.0 or later. The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

If upgrading from 3.4.x, refer to the SecurityCenter 4.0 Upgrade Guide on the Tenable Support Portal: http://cgi.tenable.com/SecurityCenter_4.0_Upgrade.pdf

Important: A new feature in this release is the availability of a standalone LCE manager to manage LCE servers separately from SecurityCenter (available for download on the LCE download page). This is intended for users who are only interested in log correlation data. If you have an LCE server that you want to continue being managed by SecurityCenter, do not install the LCE manager. The LCE manager interface operates in a similar manner to the SecurityCenter web interface but is only used to monitor and report on events (not vulnerabilities) reported by the LCE server. The LCE manager is also limited to a single organization and repository. The standalone LCE manager is licensed separately from the SecurityCenter and is licensed using the LCE license key. The LCE manager is only available for new installations and not for SecurityCenter upgrades.

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.0.3-es4.i386.rpm	2b6c862cf3703d4c46b07ad9f60a04eb
SecurityCenter-4.0.3-es5.i386.rpm	a41f7debdbb2ec64bea15b4bc5072d6b
SecurityCenter-4.0.3-es5.x86_64.rpm	7ee302076a272b3bd932aa1f4d736b38
SecurityCenter-LCE-4.0.3-es4.i386.rpm	323d888aaf27efcb739efbcf098e0ef9
SecurityCenter-LCE-4.0.3-es5.i386.rpm	d8f1716f4b246be1666c9c056a7108e9
SecurityCenter-LCE-4.0.3-es5.x86_64.rpm	49c32ab88bd6249482d1cec3ab18bab2

Changes and New Features

- User interface
    - LCE-only GUI is available when an LCE license key is used during the initial installation. If a SecurityCenter key is used, a standard SecurityCenter installation is performed.
- Scanning
    - Added "Unscanned IPs" status to Scan Results record.
    - Fixed an issue where Scan Schedules failed to launch when there were multiple organizations with same Scan ID.
- Analysis
    - The time frames to drill down on Event Queries are now locked to support LCE caching for improved performance.
    - Alphabetically sorts dropdown lists in user and group selector fields.
    - Improved Asset Summary query efficiency (requires LCE 3.6 or greater).
    - Increased query request timeout in UI from three to six minutes.
- Accept/Recast Risk
    - Allow Accept/Recast Risk rules to be applied to selection of repositories.
- Installation
    - After a LCE server addition, setup will establish/prompt for authentication with the LCE server (this may happen several minutes after the LCE server is added, towards setup completion).
- Licensing
    - Remove plugin #11933 "Do not scan printers" from counting toward the license.
- Raw Log Search
    - Increase the Raw Log Event Count (added counts of 10,000, 50,000 and 100,000).
- Reporting
    - Converted epoch timestamps in CSV exports to a human readable format.

- User Management
    - Correctly counts the number of users per role on the Role management screen.
- Miscellaneous
    - The URL path has been changed from "/sc4" to "/"; a symbolic link has been added to redirect any requests utilizing the old URL. Any custom applications using the API must be updated to use the correct path.
    - Improved performance when calculating assets, scan status and user notifications.

Hotfix01 for SecurityCenter 4.0.3 (4/28/2011)

This hotfix addresses several issues in SecurityCenter 4.0.3 including:

- Proxy fix for only sending plugins once to a daemon in multiple zones
- Better performance for scan imports
- Reduce schedule window
- Schedule evaluation occurs less frequently than previously
- Defining multiple assets bug fixed
- Flash crash fix
- Scan Timeout Increase
- Database locking fixes

File Names & MD5 Checksums:

File	MD5
SC-4.0.3-hotfix01-es4.tar.gz	2c5874510b9d98b9799b3f6e1ffd4d23
SC-4.0.3-hotfix01-es5.tar.gz	3238a14b51c916858931652cff1e6141

SecurityCenter 4.2.0 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in SecurityCenter 4.2, as well as significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

As of SecurityCenter and LCE Manager 4.2, **a new license key is required**. Please log into the Tenable Support Portal and choose to upgrade your existing license keys to SecurityCenter 4.2. If you have any issues upgrading your keys or wish to ask for a demo key for testing, please contact Tenable Support. In addition, if SecurityCenter leverages the LCE for log processing, LCE must be upgraded to version 3.6.1 for compatibility purposes.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

If upgrading from 3.4.x, refer to the SecurityCenter 4.2 Upgrade Guide.

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.2.0-es4.i386.rpm	6885f0447b6d32035aefaf7e22a1af43
SecurityCenter-4.2.0-es5.i386.rpm	2060c27ef210a770bef14520a0b0f141
SecurityCenter-4.2.0-es5.x86_64.rpm	07374a3588a5d49d3923674b2c4a9704
SecurityCenter-4.2.0-es6.i386.rpm	b506b5570cd6b96d5f85a1fedc0bb857
SecurityCenter-4.2.0-es6.x86_64.rpm	7a67a04027b256a6dc39ec3635250f97
LCEManager-4.2.0-es4.i386.rpm	f4cae872f7bd644c30f98bcfd03451c3
LCEManager-4.2.0-es5.i386.rpm	ab37d4508f39e077ec89e59a00200e81
LCEManager-4.2.0-es5.x86_64.rpm	827be253f7108f4bbb6f5fbe588a0947
LCEManager-4.2.0-es6.i386.rpm	183a3c2830859f94856bd8c883fb9c6d
LCEManager-4.2.0-es6.x86_64.rpm	5bd36a4d73ad32810208a53f2382c630

Changes and New Features

- Analysis
    - Addition of a Scratchpad for enhanced data analysis
    - New analysis tools include: CVE Summary, MS Bulletin Summary, List Software
    - Ability to set default time window for LCE queries
    - View settings: allows you to include or exclude columns in the analysis screen
- Dashboard
    - Matrix dashboard provides advanced charting
    - Sharing results of dashboard tabs
    - Import/Export dashboard tab definitions
    - Assign dashboard tabs on user addition
- Filtering
    - Asset output filtering
    - Audit file filtering for vulnerability queries
    - Enhanced filters dialog, added new filter options for: CVE ID, MS Bulletin ID, Exploit Availability, Plugin Name and CVSS Score
- Reporting
    - Custom Report Logo/Watermark image management
    - PDF Encryption with password
    - RTF output
    - Report Iterators
    - Create report while browsing underlying data
    - Reduced reporting memory consumption by utilizing temporay disk files for query results
- Scanners
    - Scanner status update button

- Scanning
  - Scan blackout windows
  - Remediation scans
  - PCI Plugin IDs 33929,33930,33931 moved from active to compliance vulnerability types for filtering
- Scan Results
  - Nessus v2 import
  - Filter based on owner (applies to reports as well)
- Repositories
  - Ability to download cumulative scan results
  - Remote repository synchronization scheduling
  - Ability to enable/disable trending snapshots per repository
- Queries
  - Ability to query for tickets, alerts and users
- Management
  - Purge individual scan results, report results and closed tickets
    - Individual Scan Results purge defaults to 365 days and it is recommend that users review the settings in System -> Configuration -> Miscellaneous -> Data Expiration
  - Added new object permissions - "Edit Organizational Asset", "Edit Organizational Policy", "Edit Organizational Query", "Edit Organizational Credentials", "Manage Report Images" and "Manage Blackout Windows"
- Miscellaneous
  - Disabled SSLv3 protocol and allowing only TLSv1 for the web server
  - The file names and locations of passive/active plugin downloads has changed

Bug Fixes

- Scanning
    - Ranges outside of zones will not cause scan to fail when using the default zone

4.2.0 Update 1 (4.2.0.1) (7/7/2011)

This update addresses several issues in SecurityCenter 4.2.0 including:

- Convert compliance pluginIDs to match local SC for remote/offline repositories
- Database locking issues
- New SC4.swf
    - Include external dependencies
    - Screen size fix for Login Banner and filter screen
    - Added limit to dropdown size and includes a scrollbar for larger lists
    - Fixes an issue when browsing to end of records
- Untar issue under ES 4 affecting plugin updates (Active/Passive pluginupdates)
- Nessus V2 file import port/server parsing issue
- Plugin Filters: Audit files not populating in the dropdown for Reports and Alerts
- Better handling of HTML special characters when generating reports
- Bug preventing some admin/tmp file cleanup
- Error message cleanup
    - Nightly cleanup job complains on ticket delete
    - Tickets - undefined variable (assigneeID)
    - Recast/Accept Risk - Deleting Rules produces undefined variable error messages
    - Removes PHP notice and warning when editing a report that contains an iterator
    - Removes PHP notice when editing a role
- Configuration database: Passive plugin type and Suffix correction
- New debug script

4.2.0 Update 2 (4.2.0.2) (9/19/2011)

This update is cumulative to include changes from 4.2.0.2 and addresses several issues in SecurityCenter 4.2.0 including:

- Apache HTTP Server upgraded to version 2.2.21 - (CVE-2011-3192) Apache httpd Byte Range Filter DOS.
- Addresses an issue when Copying scan policies with attached files
- Added a User-Agent header for plugin authentication
- Better handling of HTML special characters when generating reports
- Startup script properly handles stale PIDs for Jobd and lightning-proxy
- Online Help System improvements

File Name & MD5 Checksum:

File	MD5
SC4.2.0.2_Update_Package.tar.gz	3eda58c261799a4ccffb3ad32da7e91a

SecurityCenter 4.4.0 Release Notes - 4/17/2012

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following list describes many of the changes that are included in SecurityCenter 4.4, as well as significant issues that have been resolved and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.0.0 and later. Users upgrading from 3.4.x must first perform an upgrade to SecurityCenter 4.2 before attempting to install version 4.4. Refer to the SecurityCenter 4.2 Upgrade Guide.

SecurityCenter now only supports Nessus scanners 4.2 or later. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

As of SecurityCenter 4.2 and LCE Manager 4.2, **a new license key is required**. If these products are being upgraded from a release prior to 4.2, please log into the Tenable Support Portal and choose to upgrade your existing license keys. If you have any issues upgrading your keys or wish to ask for a demo key for testing, please contact Tenable Support.

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.4.0.3-es4.i386.rpm	[ded7110efa8b3248d4b90926eec85334]
SecurityCenter-4.4.0.3-es5.i386.rpm	[adafcfafbaa54627e0ca4615b016010b]
SecurityCenter-4.4.0.3-es5.x86_64.rpm	[a49dfabc97a7707a8c8d9ab29bc4d78a]
SecurityCenter-4.4.0.3-es6.i386.rpm	[ddf9065116f112990876204501456351]
SecurityCenter-4.4.0.3-es6.x86_64.rpm	[cb09710e759a287c9bb15b12cb9eb08f]
LCEManager-4.4.0.3-es4.i386.rpm	[d1fab3f74529ea3369714f2a23a600f1]
LCEManager-4.4.0.3-es5.i386.rpm	[b8c89df56535851643e33f2d6632ea32]
LCEManager-4.4.0.3-es5.x86_64.rpm	[d995774fb63cc2c207fb8849444b0240]
LCEManager-4.4.0.3-es6.i386.rpm	[ae1e884db497f9e834169a9c3a40c48f]
LCEManager-4.4.0.3-es6.x86_64.rpm	[002f48884481bea280688769845f538d]

Changes and New Features

Scanning

- The scan proxy has been deprecated: SecurityCenter now utilizes the Nessus XMLRPC API to communicate to scanners. During the upgrade process, all defined scanner ports will be changed from 1241 to 8834, which is the default web server port for Nessus 4.2 and above.

  > **Note:** if you have any firewalls between your SecurityCenter and Nessus scanners, the rules may need to be updated for the new port.

- Supports scanning by hostnames: Scan Targets can be entered as IPs or FQDNs

- Scanning of Virtual Hosts: supports up to 256 unique hostnames on a single IP address. A "node" is uniquely identified by the IP + hostname pair (meaning in the IP Summary tool, each IP + hostname pair will return as a separate record).
- Added Nessus v2 export: now has download options for both v1 or v2 format (deprecating the .NSR format)
- Added the Nessus "Informational" Severity: SecurityCenter now displays 5 levels of severity: Info, Low, Medium, High, Critical
- Ability to integrate with the Tenable Nessus Perimeter Service for outside-in scanning from the cloud.

Assets

- New Static Asset type to support hostnames: Names are resolved to IP addresses on Add/Edit and updated during a nightly job.

Vulnerability Analysis

- New analysis tools included: IAVA Summary and DNS Name Summary
- Added the ability to set a default filter for vulnerability queries. This allows users with a large number of repositories to limit the initial query when first loading the screen.
- New vulnerability display filter options for DNS Name and IAVA ID

Event Analysis

- LCE Search Bar: a search bar that provides quick access to the current or active filter
- Custom IP links added to the right-click context menu for easy access (for List of Events and IP Summary tools)

Reporting

- New 'Quick Report' allows users to quickly create and run a template report with default values
- Support 'Iterator' for DNS Name
- Import/Export Report Template definitions

Dashboard

- Ability to export individual dashboard components as PNG images from the component menu
- Explicit Schedules for dashboard evaluation

Repositories

- Ability to download cumulative scan results in Nessus v2 format
- Can now synchronize remote repositories allowing an n-tiered environment

Management

- Displays scanner status, scanner, and web server version on the Scanner page
- Scanner Plugin Set is now displayed on the Scanner Detail screen
- Added a button to manually refresh scanner status
- Added an Enable/Disable button in the scanner definition. Disabled scanners will not be used in scans and plugins will not be pushed to them, but their status will continue to be updated.
- Now possible to upload authentication certificates for each scanner, rather than having one certificate for all scanners.
- Option to verify the certificate. If enabled, verifies the certificate's CA, checks the existence of a Common Name (CN) in the certificate, and verifies that it matches the hostname provided.
- Supports Smartcard or SSL Client certificate authentication of users
- Added filtering to the Job Queue display page
- New Diagnostics screen that displays system status and collects diagnostic information

Bug Fixes

- Improved database concurrency issues that were resulting in 'database locked' errors
- Significantly reduced plugin synchronization time and system load impact
- Improved query performance when using a large number of repositories
- Improved performance when loading the Host Detail screen
- Optimized trend queries to only perform differential queries
- Removed timeout on LCE Event Analysis screens

- Enabled TCP port scanner and allow for port selection in remediation scans
- Many other minor improvements and bug fixes

Third-Party Dependency Changes

- Upgraded the following dependencies to the specified versions:
    - Apache httpd 2.2.22
    - PHP 5.3.10
    - OpenSSL 0.9.8w
    - SQLlite 3.7.10
- New dependency added:
    - libcURL 7.24.0

4.4.0.3 (6/20/2012)

New Features/Improvements

- Added Proxy support for Perimeter Service scanners
- Improved prepareassets performance during scan import/asset calculation
- Increase the default ScannerStatusTimeout setting from 60 to 120 secs
- Allow for multiple values in CVE, MS Bulletin, and IAVA filters
- Add support for DOD Classification Markings in Report Headers and Footers
- Add support for IAVB and IAVT references, renamed the existing "IAVA ID" filter to "IAVM ID"
- Disabled SSLVerifyClient "optional" setting for new installs
- Apache httpd.conf Options directive changes for improved security
- Set the Analysis page to not load all the information at once, this reduces the time to load
- Removal of the initial password of an account when a ssl client certificate is associated
- Locking of Admin user accounts exceeding maximum login attempts
- Upgraded the PHP version to 5.3.14 and OpenSSL to 0.9.8x

Bugs Addressed

- Fixed the scanProgress database lock error that occurred during concurrent scans
- Reordering of Dashboard Tabs was not retained when you logout and log back in
- Better formatting of the .csv report when the 'Plugin Output' field is very large
- Report Iterator IP Info failure
- Fixed a crash in the generatenessus tool when extracting os name from plugin output
- Mitigation not occurring in some cases on import
- Setting the max_hosts to a number smaller than 4 caused scan problems
- ActionScript error when attempting to add users
- Prepareassets not clearing out the AssetIPCount table correctly, which could cause slowness on the Asset screen
- Prevent multiple scanner update jobs from occurring simultaniously
- User Screen Manager filter incorrectly populated
- Post Scan processing setting was not always saved correctly

SecurityCenter 4.6.0 Release Notes - 12/4/2012

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This document describes many of the changes that are included in SecurityCenter 4.6, as well as significant enhancements and notes for upgrading. A PDF file of these release notes is also available here.

Upgrade Notes

Upgrades are only supported for those users running SecurityCenter 4.2.0 and later. Users upgrading from 4.0.x must first perform an upgrade to SecurityCenter 4.2 or 4.4 before attempting to install version 4.6. Please refer to the SecurityCenter 4.2 Upgrade Guide or SecurityCenter 4.4 Upgrade Guide for information about upgrading to SecurityCenter 4.2 or 4.4. Information about upgrading from SecurityCenter 4.2.0 and later is available in the SecurityCenter 4.6 Upgrade Guide.

SecurityCenter now only supports Nessus scanners 4.2 or later. In addition, if SecurityCenter leverages the Log Correlation Engine (LCE) for log processing, the LCE must be running a minimum of version 3.6.1 for compatibility purposes.

The command syntax for an RPM upgrade is as follows:

```
# rpm -Uvh [RPM Package File Name]
```

File Names & MD5 Checksums

File	MD5
SecurityCenter-4.6.0.1-es5.i386.rpm	[232dabca6bc46c8fc1cc1209146ba7b0]
SecurityCenter-4.6.0.1-es5.x86_64.rpm	[191d1f4308f53d4942e152c7b35da6c0]
SecurityCenter-4.6.0.1-es6.i386.rpm	[a3dd0892c14fdf9871fbfd871fc3cbe3]
SecurityCenter-4.6.0.1-es6.x86_64.rpm	[b5a2629b241a0e29f05413149a1a093f]
LCEManager-4.6.0.1-es5.i386.rpm	[09dc5bcdcff972c32016ccfbf8501904]
LCEManager-4.6.0.1-es5.x86_64.rpm	[b6d808d2dc3fa2ffcf991319268c143d]
LCEManager-4.6.0.1-es6.i386.rpm	[b9c8abd7d36ec754b5c448766bbfb064]
LCEManager-4.6.0.1-es6.x86_64.rpm	[9f6ab55073aea62829382bd0dc1af294]

Changes and New Features

General

- **Improved search functionality in drop-down lists** – A "smart" control has been added throughout the application that allows users the ability to type in text within a drop-down list that instantly starts returning results as they type.

Scanning

- **IPv6** – Full support for IPv6 scanning. This includes the capability to:
    - Perform an IPv6 host discovery scan
    - Passively detect IPv6 hosts
    - Scan a single IPv6 host
    - Scan a whole range of IPv6 addresses (up to the equivalent amount of addresses of a Class A network).

  - Scan Assets defined with IPv6 addresses
  - IPv6 based scan results can apply all the same functions and features as IPv4 network scan results
- **Detailed Scan Progress Bar** – The new, detailed Scan Progress bar provides a visualization of the progress of current scans, as well as other statistical information about the status of a scan. SecurityCenter also now provides in-scan details of where the IP addresses are going (to which scanners) and the progress of individual chunks, etc.
- **Support for new Juniper and CheckPoint firewall compliance checks** – The ability to define and report on the new Juniper and Check Point firewall compliance Nessus plugins has been added.
- **Support for setting preferences for Cisco IOS compliance checks** – SecurityCenter allows users the chance to set preferences when performing Cisco IOS compliance checks. This includes the ability to audit the "Saved", "Running", and "Startup" configurations.

Assets

- **Asset LDAP queries** – SecurityCenter 4.6 provides the ability to connect to an LDAP directory (i.e., Active Directory) and pull host information in for use with a scan policy. This new functionality expands what SecurityCenter can do when creating Asset lists. This allows customers to leverage existing infrastructure in ways to help streamline the use of SecurityCenter.
- **Asset Calculator** – The Asset Calculator enhancement changes the way a user can create Assets by providing the flexibility to manipulate how existing Assets are leveraged. Previously, when creating a new Static Asset, the user had the option to "Copy" addresses from Assets on the right into the text area on the left, which caused the function to be called on every Asset list. This enhancement provides users the ability to utilize the following methods when selecting multiple assets:
  - Union: Combines addresses from Assets on the right with addresses on the left, removing duplicates.
  - Intersection: Removes all addresses from the left that are not present in the selected Asset lists on the right.
  - Difference: Combines addresses from selected assets on the right with addresses on the left, and then removes any addresses that were in both.

- Complement: Removes all addresses from the left that are present in the selected Asset lists on the right.

Management

- **Support for StartTLS for LDAP** – Support for StartTLS allows SecurityCenter to encrypt its use of LDAP without using LDAPs. StartTLS is an extension that allows you to take previously clear text/unencrypted protocols and encrypt them.
- **Optimize Plugin updates** – The optimization of plugin updates greatly decreases the amount of time it takes to do large-scale updates (for example, after a new install).
- **Classification Banners** – This feature allows users to set a banner on the top and bottom of the web user interface as well as reports. The banners state the classification of the data represented on the screen or in the report. Some examples of classifications are "Top Secret" and “Secret”.
- **Support CoSign authentication** – SecurityCenter 4.6 introduces a new server authentication method that uses the open-source CoSign single sign-on solution.
- **LCE client-management** – SecurityCenter 4.6 provides the capability to manage LCE clients from the SecurityCenter management interface. This provides a much more efficient method to tune how events are generated via the LCE.
- **Log all credential changes at the Organizational level** – All add/change/delete actions on "Credentials" are now logged in the admin log.
- **Perimeter Service scanner/SC proxy support** – Users now have the ability to use SecurityCenter's proxy server information when connecting a Nessus Perimeter Service scanner or other Nessus scanner which resides on the other side of a proxy server to SecurityCenter.
- **Remove password of account associated with a certificate** – To meet PKI requirements, it is now impossible to log into an account that has a certificate associated with it. When creating an account to authenticate via a certificate, the "password" box is removed.
- **New "Update Status" button for PVS** – There is now a button that allows users to perform a manual status check of each PVS that would trigger an update of a report, if one is available.
- **Add support for NTLM web proxy authentication** – The NTLM web proxy authentication feature enables SecurityCenter to authenticate to a proxy server using NTLM.

- **Tool to remove duplicate namedb entries** – A new tool was introduced that removed duplicate MAC addresses, DNS, and NetBIOS name entries in the namedb for each repository.
- **Command Line utility that enables the import/export of repositories** – This utility provides the ability to perform offline Import/Export functions from the command line.
- **Can now create a sanitized debug output** – There is now a command line tool that can be run against a standard debug output that will remove IP address and password information before sending the debug report to Tenable Support.
- **Added Notification of unsuccessful login attempts** – Added the capability to notify users on login of date and time of the user's last unsuccessful login, IP address of the user's last unsuccessful login, date and time of the user's last successful login, IP address of the user’s last successful login, and number of unsuccessful login attempts since the last successful login.

Dashboard

- **HTML5 read-only dashboard** – The HTML5 read-only dashboard is the first step in the SecurityCenter's front-end redesign.
- **Default Dashboard Components** – SecurityCenter 4.6 introduces a "default" dashboard. This provides users a basic template to view data as it comes in and build a more tailored dashboard from that foundation. Please refer to http://blog.tenable.com/sc4dashboards/ for additional dashboard examples.

Reporting

- **Generate a report at the end of a scan** – This feature provides the ability to generate a report based specifically on a particular scan rather than utilizing cumulative data.
- **Additional plugin fields in CSV reporting** – This feature adds the ability to take specific fields that were present in "Vulnerability Details" (i.e., Solution, Description. CVE, etc.), and make them available as separate columns in a CSV export/report.
- **Generate a report on an Alert** – Reports can now be generated from an Alert based on any query you set for vulnerability, PVS, or LCE data. This feature automates much of the incident response process as a pre-canned report. This feature also provides coverage of various events from different log sources and also vulnerability and system data generated via scans, patch audits, and passive discovery.

- **Report Results Sharing** – The Report sharing feature introduced in SecurityCenter 4.6 allows a user to select a report from the list, click the share button, and select a SecurityCenter user from the list. Once shared, it shows up on the selected SecurityCenter user's list of reports within SecurityCenter. This keeps the report within SecurityCenter, and not sent to an email address hosted on a server that is not intended for the sensitive information that may be contained the report.
- **Report Filter Find/Replace** – The Report Filter Find/Replace enhancement enables users to quickly and easily update query filters across an entire report instead of manually editing each element in every chapter of the report.

Vulnerability Analysis

- **Nessus Scan Policy Import/Export** – This new feature allows users to create a policy within SecurityCenter, export it, and then upload it to another SecurityCenter or a standalone Nessus server. You may also upload policies created on a stand-alone Nessus server into SecurityCenter.
- **Support for Plugin Date Filters** – This feature allows users to filter on the date associated with the plugin. There are five pre-defined ranges (e.g., "within the last week") that the user can filter on based on the dates of plugins.

Event Analysis

- **Added "And/Or/Not" filter options for Event queries** – Users now have the ability to filter out events using "And/Or/Not" expressions in the Event Analysis Tool. Previously, raw log searches would have to be performed to accomplish this task.
- **Ability to create Alerts from raw log events** – There is now the capability for users to create an Alert based on data from raw log events gathered from the Log Correlation Engine.
- **Added "Start/End" time range setting to raw log queries** – Users can now set a start and an end time when searching through the raw logs gathered by the Log Correlation Engine.
- **Enhanced querying of archived LCE data** – This feature allows users to enter a date for querying, instead of having to scroll through a list to find something closer to the current day.

Bug Fixes

- Removed a memory leak that would occur when editing report templates repeatedly.
- Resolved the issue where the "prepareassets" function only partially loaded the .db and .raw if the file size was over 2GB.
- Fixed an issue where saving an Asset fails if creating it from a filter containing multiple lines.
- Fixed an issue where a user was not able to upload a compressed Nessus file of a repository to SecurityCenter.
- Modified the "Email on Ticket Assignment" function. Previously, it would not fire an email when a ticket was created via an Alert.
- Resolved an issue where the "Post Scan" setting for the number of days was not displaying correctly.
- Fixed an issue where sorting Asset Lists by IP count was incorrect after a screen refresh.
- Fixed an issue where the SecurityCenter start script failed after adding a custom CA certificate.
- Fixed an issue where deleting a user with shared credentials deleted the credentials for all the users.
- Resolved the major issue of scans failing due to the database locking under certain conditions.
- Many other minor improvements and bug fixes.

4.6.0.1 (12/13/2012)

Bugs Addressed

- Fixed an issue where IPs that appear in multiple repositories are getting counted multiple times toward license
- Fixed an error when exporting CSV from vulns page when filtering on a repository
- Fixed an issue where credentials from the HTML interface where logged in cleartext

Security Center 3.0.4 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Version 3.0.4 of Security Center is a maintenance release. Issues reported or discovered since the release of v3.0.3 have been addressed. Highlights of the changes include:

- Greater integration and support of the Compliance Checks features of Nessus
- Time to generate the "All Assets" list is significantly reduced in all locations
- System security enhancements
- System wide ease of use changes
- Improvements in working with the Cumulative Vulnerabilities DB
- Enhanced Thunder query response times
- Red Hat Enterprise Server 4 support
- Red Hat ES 4 SELinux is supported using a Targeted Policy

Security Center 3.0.5 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

This release includes about 40 bug fixes of varying severity. If you are working with our support group and they have advised you to upgrade to 3.0.5, you should do so at this time. Also, if you are running SC3 on Red Hat ES4, you should upgrade to 3.0.5 as three separate tickets were related specifically to ES4 issues.

The major issues fixed in SC 3.0.5 include:

- Higher performance of each users' AllAssets list
- Performing active scans with > 254 asset groups
- IDS event filters for Dragon events would crash the logd process
- A variety of ES4 specific issues
- Scan polices now have support for the "Max number of packets per second for port scan" setting
- LCE queries and report graphs are more accurate

Security Center 3.0.6 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Version 3.0.6 of Security Center includes corrections with regard to the following:

- Vulnerability date/time stamps
- Display issues while viewing the cumulative vulnerability database
- Active scanning issues
- Viewing/display of IDS data
- Minor issues with reporting

Security Center 3.0.6 Hotfix01 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

As part of QA testing of version 3.2, Tenable has discovered an issue with recurring scans generation that also affects version 3.0.x. The issue is that when the next occurrence of a scan is scheduled, only the day and month will be incremented, but not the year. If the year should have been advanced, this will result in scans that are scheduled to run far in the past.

Any recurring scans that have already run and have not had the year increment properly must be edited manually. To resolve this issue for recurring scans that are yet to run and have the year incremented, please install Security Center 3.0.6 Hotfix01.

The hotfix is operating system specific, please be sure to obtain the correct package for your Security Center system (Red Hat ES 3.x or ES 4.x).

To install the files:

- Transfer the hotfix package to your Security Center system.
- Extract the files to a temporary directory using the command:
  tar xvfz <Hotfix01 Package File Name>
- A directory will be created under the extraction directory, change to this new directory.
- Run the install.sh file that is in the newly created directory

The installation script will perform the following functions:

- Stop the SecurityCenter service
- Backup (copy) /opt/sc3/daemons/lightningd
- Copy the new lightningd file into place
- Verify the new file's permissions
- Restart the SecurityCenter service

There is also a text file included in the package that will provide additional information.

SecurityCenter 3.2 Release Notes

This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

SecurityCenter Version 3.2 introduces several significant features as detailed below, as well as many minor changes and bug fixes.

Reporting

The reporting module has been significantly upgraded again, new features include:

- There are now a significant number of basic and advanced pre-configured reports
- Management of reports in-progress has been added
- There is now a Summary by Asset List reporting chapter
- Selection of multiple vulnerability severities is now possible when defining a report
- The ability to select multiple asset lists when defining a report has been added
- Intersection or Union may be chosen when multiple asset lists are selected for a report

CSV Output from Queries

It is now possible to export queried Security Center data in comma separated values (.csv) format from the Cumulative Vulnerability Database, Analyze IDS Events, and Analyze Logs screens.

LDAP/Active Directory Integration

Support for integrating with a single LDAP or Windows Active Directory for user authentication has been added. The integration allows for a mixed model, utilizing both Security Center's authentication mechanism (TNS Auth), as well as an LDAP/Active Directory (LDAP). Authentication is configured on a per-user basis, allowing for each user account to be assigned either TNS Auth or LDAP at any one time.

Miscellaneous

There are several improvements to asset list functionality; most notable is the ability to perform bulk uploads of static asset list ranges.

It is now possible to configure and maintain multiple compliance checks *.audit* files for a single scan policy.

SC3 now provides a mechanism for locking user accounts manually, or based on logon attempt failures.

SecurityCenter 3.2.1 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

The following changes are included in SecurityCenter 3.2.1:

Cumulative Vulnerability DB

- Added support for plugin ID #24760, Windows File Contents Check.
- Asset List filter returns results properly for large asset list names.
- Corrected PVS OS Detection events in SC3 that were displaying with special/control characters.
- CSV row output hard limits have been removed.
- Corrected URL's for drill down failing to work when using the List OS Tool for large OS descriptions.

Analyze IDS Events

- Cisco IDS base64 decode now works in LSF mode.
- CSV row output hard limits have been removed.

Analyze Logs

- Fixed issue with reset of filter settings.
- CSV row output hard limits have been removed.

LDAP/Active Directory Support

- LDAP TLS support now works.
- "Size Limit Exceeded" error when Check Settings clicked has been corrected.
- Security Center now permits empty Username and Password LDAP fields (anonymous binds).

Scanning

- Very large scans now import without issue.
- Dynamic Asset List updates can now be configured to run during scan import, during nightly processes or manually only.
- SSL authentication between SC3 and Nessus is now available.
- A condition which would sometimes cause IP addresses to be scanned multiple times during the same scan has been corrected.
- A condition which could cause a scan import failure has been corrected.
- Entries in a particular order would cause IP's in the Do Not Scan List to be scanned anyway. This has been corrected.

Reporting

- Reports use proper data sets for the user running the report.

Miscellaneous

- Support added for maximum authentication attempts and locking an account if this is exceeded.
- A number of trivial text and screen formatting issues have been resolved.
- SC3 will now properly handle asset lists that contain ranges of IP's using A.B.C.D-N format.
- The reason for accepting risk is now displayed for the appropriate vulnerabilities when viewing vulnerability details.

SecurityCenter 3.2.2 Release Notes

> This release is end-of-life (EOL). Upgrade to a supported version. For information about EOL dates and policies for Tenable products, see the Tenable Software Release Lifecycle Matrix and Policy.

Immediately after the release of SecurityCenter 3.2.1 Tenable noticed that there was an issue related to running certain types of scans in the product. While many users will never encounter the problem, it is significant for those that will encounter it, so we chose to fix it immediately. For this reason version 3.2.2 is being released.