Tenable Cyber Exposure Study – Vulnerability Management

Last Revised: December 06, 2023

Copyright © 2023 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.

Table of Contents

Overview

Vulnerability Management (VM) is a proactive approach to identify, manage, and mitigate vulnerabilities to improve the security of enterprise applications, software, and devices. The approach involves identifying vulnerabilities in IT assets, evaluating risk, and taking appropriate action across systems or networks to remediate these vulnerabilities.

Ideally, this means proactively scanning the environment looking for vulnerabilities and systematically patching the identified vulnerabilities as they are found. However, the process is rarely as simple or straightforward as that. A solid vulnerability management program is important for several reasons:

Security: A good program helps organizations identify and address weaknesses within their IT infrastructure. By proactively identifying and mitigating vulnerabilities, organizations can reduce the risk of breaches and cyber attacks.

Compliance: Many regulatory requirements and industry standards require organizations to have a vulnerability management program in place. For example, the Payment Card Industry Security Standard (PCI-DSS) and the Health Insurance Portability and Accountability Act (HIPAA) all mandate regular vulnerability assessments and remediation.

Risk Reduction: By regularly assessing and mitigating vulnerabilities, organizations can reduce their exposure to potential threats and the associated financial and reputational risks.

Operations Continuity: Vulnerabilities can lead to system failures and unscheduled downtime, which are disruptive to business operations. Identifying and mitigating vulnerabilities before they can be exploited maintains continuity and avoids costly disruptions.

Data Protection: Protecting sensitive data from unauthorized access, disclosure, or theft is paramount in avoiding data breaches that can potentially incur legal and financial consequences.

Cost Savings: The cost of addressing vulnerabilities is typically much lower than the cost of dealing with a security breach.

Compliance with Best Practices: The implementation/adoption of a vulnerability management program aligns with common industry standards and best practices such as ISO 27001, NIST, and the CIS Critical Security Controls (CIS Controls). These standards and practices ensure vulnerabilities are monitored and addressed.

The fact remains that there are many questions to be considered when dealing with vulnerabilities. The most important is where to start. Begin with creating a solid vulnerability management

program. Take a proactive approach to identify and address vulnerabilities before they are exploited vs. taking a reactive approach by responding to security incidents after they occur.

What type of VM program does the organization currently have? Most organizations fall into one of the following three types: Headline driven VM programs have a drop everything and fix {current headline vulnerability here, such as “Log4J”, or “Heartbleed”} approach. Compliance driven VM programs tend to pick a compliance program (NIST) and start at the top and work their way down. Qualitative driven programs tend to focus on a particular set of vulnerabilities, such as let’s fix all the database vulnerabilities this month, or lets address all the Microsoft vulnerabilities before any others.

There are benefits and concerns with each of these types and Tenable can help by tying the organization's VM program to Cyber Risk with Risk-Based Vulnerability Management (RBVM). Legacy VM programs tend to address traditional IT assets only, they are reactive and only check the minimum compliance boxes. RBVM prioritizes vulnerability data with threat intelligence, delivers dynamic continuous visibility of the entire attach surface, and is proactive. Proactively staying ahead of emerging threats keeps systems and data more secure, prevents data breaches, and avoids costly disruptions.

Risk-Based Vulnerability Management

Risk-Based Vulnerability Management (RBVM) is a process that reduces vulnerabilities across the attack surface by prioritizing remediation based on the risks they pose to the organization. Unlike legacy vulnerability management, risk-based vulnerability management goes beyond discovering vulnerabilities, by helping organizations understand vulnerability risks, by introducing threat context and insight into potential business impact.

RBVM uses machine learning to correlate asset criticality, vulnerability severity, and threat actor activity. This helps organizations cut through vulnerability overload so teams can focus on the relatively few vulnerabilities that pose the most risk to the enterprise. Legacy vulnerability management solutions weren't designed to handle the modern attack surface and the increasing threats.

The attack surface is no longer just traditional IT assets. Included are mobile devices, web applications, cloud infrastructure, containers, Internet of Things (IoT) devices, and operational technology (OT) assets. In these modern networks, legacy vulnerability management tools can’t deliver complete and timely insights into all of the devices across the entire attack surface. This leaves uncertainty and increases Cyber Exposure. Instead, these legacy tools are limited to a theoretical view of the risk a vulnerability could potentially introduce, which can cause security teams to chase after the wrong issues while missing many of the most critical vulnerabilities posing the greatest risk to your business.

What’s even more frustrating are the mountains of vulnerability data generally returned from legacy vulnerability management processes. How do organizations identify which vulnerabilities to fix first? How do administrators know which weaknesses pose the greatest threats to the organization?

RBVM eliminates guesswork, by taking a risk-based approach to vulnerability management, security teams can focus on the vulnerabilities and assets that matter most and address the organization’s true business risk instead of wasting valuable time on vulnerabilities attackers may not likely exploit. If you’re new to risk-based vulnerability management, check out this comparison guide. The guide breaks down the differences between legacy vulnerability management and risk-based vulnerability management with insight into how a risk-approach can make your organization's vulnerability management program more efficient and effective.

With the principles of Cyber Exposure Management in mind, dashboards, such as the InfoSec Team - One Stop Shop Comprehensive Attack Surface dashboard for Tenable Security Center helps the organization team maintain a high level of awareness and vigilance. The filters and components are

tailored to guide teams in detecting, predicting, and acting to reduce risk across their entire attack surface. Information security teams are empowered to analyze findings, remediate identified risks, track progress, and measure success against the organization's charter and SLAs.

Organizations often have teams that focus on the detailed information relevant to the teams' assets; or operational focus areas, such as Windows, Linux, databases, or network infrastructure. The InfoSec Team – One-Stop Shop Comprehensive Attack Surface dashboard, shown in the following image, contains components that do not require specific asset list filters to be applied before use.

However, organizations with teams that focus on a specific group of assets benefit from using custom asset lists. Information security teams can visualize findings against assets that are "owned by" or "assigned to" specific teams within the organization using this method. Additionally, an Output Assets filter can be set to provide greater insight into where additional resources need to be allocated to mitigate vulnerabilities.

The Output Assets filter is only available when using the Asset Summary Tool. When this tool is selected, you have the option to refine the filters to include specific Asset information.

For Tenable Vulnerability Management, dashboards such as the Vulnerability Management Program Health dashboard shown in the following image, helps security operations teams ensure their scanning program is appropriately maintained for an evolving operational technology landscape aligned with business strategy.

There are many factors that can adversely affect the scope and accuracy of scan data, such as failed credentials, network problems, or license limitations. This dashboard provides security analysts comprehensive information to monitor the health of their scanning program.

Analysts can drill into the summary information displayed in the dashboard to troubleshoot upstream scanning problems that can adversely impact downstream reporting to stakeholders.

Patch Management

The primary objective of a patch management program is to prioritize vulnerabilities based on the full business context, including a comprehensive analysis of vulnerability characteristics and criticality rating for each asset.

Not all vulnerabilities are created alike. Some pose an immediate risk to the organization, while others pose little to no risk at all. The problem with legacy vulnerability management practices is that they rely solely on Common Vulnerability Scoring System (CVSS) ratings to prioritize remediation. CVSS returns mountains of vulnerability data—with many rated “critical” or “high,” even if they don’t pose an actual risk to the organization.

> **Note:** Few organizations have the resources necessary to remediate every vulnerability across their attack surface. Once organizations have discovered and assessed all of their assets, analysts will need to gain insight into the nature and severity of each vulnerability so these vulnerabilities can be prioritized. Remediation and mitigation plans should be created based-off prioritization plans.

Most legacy methods employ the CVSS to prioritize which vulnerabilities to remediate first. For example, a typical organizational policy is to remediate all vulnerabilities with a CVSS score of 7 and above. This method has become commonplace among most security teams, yet it’s proven to be inefficient and ineffective when taken in isolation. This is because while v3 of CVSS has certainly made some improvements over past versions, CVSS still suffers from significant problems — not least of which is the fact its risk unaware. Since most CVSS scores are assigned within two weeks of vulnerability discovery, the score only employs a theoretical view of the risk a vulnerability could potentially introduce. This leads security teams to waste the majority of their time chasing after the wrong issues, while missing many of the most critical vulnerabilities posing the greatest risk to the business.

Another major problem is that most teams only use the CVSS base score which never changes, irrespective of the changes in the threat landscape. That’s because the base score doesn’t have any degree of context from which to understand the actual risk a vulnerability poses to the business. While CVSSv3 introduced environmental and temporal scores to supplement the base score, these two additional components are often difficult to understand and haven’t proven to be terribly effective for measuring risk. As a result, the majority of organizations opt to simply continue to use the base score exclusively.

Understanding which assets are affected by critical vulnerabilities is as important as locating the vulnerabilities themselves. However, the combination of the organization's most important assets,

along with having those assets contain high risk vulnerabilities, makes patching these assets the highest priority. For example, if a vulnerability was identified with a criticality rating of 9.0 (on a scale of 1 to 10, with 10 being the most severe) on a secondary file server. However, should the same vulnerability occur on a server that houses all the companies financial and sensitive customer information, the latter should take a higher priority and be patched first.

Identifying assets running EOL applications is an important part of assessing and minimizing organizational risk since patches, updates, and security fixes are no longer available. The Center for Internet Security (CIS) states that organizations must ensure only software applications or operating systems currently supported and receiving vendor updates are added to the organization's authorized software inventory. Organizations need to tag all unsupported software in the asset inventory.

The Cyber Risk Executive Briefing dashboard for Tenable Security Center assists cyber security leaders who are building or strengthening a vulnerability management program to better visualize the modern attack surface.

The Information presented focuses on the findings organizations should prioritize and mitigate first, by leveraging the Vulnerability Priority Rating (VPR). The VPR score is an output of Predictive Prioritization, which allows cyber security leaders to focus on items that help drive key performance indicators, by combining research insights, threat intelligence, and vulnerability ratings to reduce noise. Effective vulnerability remediation becomes easier as vulnerabilities are presented in a manner that helps visualize vulnerability remediation programs and provide measures against established goals and SLAs.

The prioritized data establishes a measurable reference point used by cyber security leaders to create actionable mitigation tasks based on VPR and improve the risk reduction timelines. When not using VPR as a filter to focus on the most significant concerns, noise increases and the large number of critical and high vulnerabilities, as determined most often by Common Vulnerability Scoring System (CVSS) rating, become cumbersome and difficult to sort. The dashboard is laid out to provide a high-level risk summary in a visual manner allowing business leaders to gain insight into their vulnerability management programs quickly and effectively. Risk is measured between customer lines of business, locations, etc. and fosters healthy team competition to not be at the top of the proverbial wall-of-shame.

Key areas of concern are unsupported products, asset management/vulnerability remediation, and secure communications for sensitive information. Tenable Vulnerability Management helps to address these issues with the Fundamental Cyber Hygiene Report Card dashboard.

A recent publication from the U.S. Cybersecurity Infrastructure Security Agency (CISA) outlines their Strategic Plan FY2023 - 2026 to provide a vision for the future of cybersecurity and helps to ensure technology products are safe and secure by design. This dashboard provides an overall picture of an organization's fundamental cyber hygiene. The three goals identified in the Strategic Plan FY2023 - 2026 plan are:

- Address Immediate Threats
- Harden the Terrain
- Drive Security at Scale

Unsupported products, operating systems, and applications are a major cause of data breaches. The proliferation of unsupported and end-of-life (EOL) products is a common security problem experienced across all organizations. As applications and operating systems reach EOL, vendors stop offering support, causing security and stability to decrease over time. A comprehensive summary of unsupported products in the environment is provided via the Top Unsupported Product widget within the dashboard.

Another major concern is visibility into the assets in the environment and how effectively vulnerabilities on those assets are managed. As vulnerabilities are identified, remediation must be prioritized and tracked in accordance with organizational goals and Service Level Agreements (SLAs). Reviewing remediated vulnerabilities and the remediation timeframe provides valuable information to the organization on the effectiveness of the risk remediation program. Vulnerabilities that are known to be exploitable are particularly dangerous, since there are exploit frameworks readily available to exploit them. Details are included on vulnerabilities where a patch to remediate the exposure was available more than a year ago.

Data on secure communication controls for sensitive information is provided within the Fundamental Cyber Hygiene Report Card dashboard. The status on SSL certificates that are aged out or soon to be aged out is displayed, along with SSL and TLS insecure communication exposures in the environment. Information about exposure of various types of potentially sensitive information is provided. Many organizations are unaware how much sensitive information is exposed, which enables attackers to tailor an attack path specifically targeting the organization, leading to data loss exposures.

Operating System and Application Patch Management

Tenable Vulnerability Management enables organizations to continuously assess the health and security posture of the network, including identification and monitoring of unsupported software. Quick identification of unsupported operating systems and applications enables risk managers to see risks associated with EOL software. Identifying exposures provides the operations teams direction to implement, act, and prioritize remediation efforts to mitigate cyber risk. Risk managers and operations teams can communicate to the leadership team how upgrading unsupported operating systems and applications reduces their network risk.

Tenable Vulnerability Management uses active methods to identify EOL products found in the environment by examining the Microsoft registry, common software installation locations, or using applications utilities such as YUM or APT in Linux systems. Risk managers are able to verify the operation team's activities and identify areas for risk mitigation.

The Unsupported Software dashboard for Tenable Vulnerability Management provides the organization with a clear and simplified method to identify EOL software and enables security managers to predict where risk will increase and develop a mitigation plan.

The Unsupported Product Summary dashboard for Tenable Security Center, shown in the following image is similar to the Unsupported Software dashboard for Tenable Vulnerability Management and consists of seven components that report on unsupported (end-of-life) products found in the environment. Components include indicators, bar graphs, pie-charts, and tables to display, track, and report on unsupported operating systems and applications.

The Historic Patch Mitigation Status dashboard for Tenable Security Center monitors vulnerability mitigation on an organization’s network in order to help security teams understand the effectiveness of their patch management efforts. Increased visibility into vulnerability mitigation can assist security teams in implementing improved patch application procedures as needed.

By monitoring the patterns of patch application and vulnerability mitigation, security teams can better understand the effectiveness of their efforts and make adjustments as necessary in order to effectively secure their network.

The components in this dashboard display data about the mitigation dates of detected vulnerabilities. Two filters are leveraged: “Days to Mitigate” and “Days Since Mitigation.” The components depicting patch rates use the “Days to Mitigate” filter to count vulnerabilities that were mitigated within the specified number of days of initial discovery. The count is based on the difference between the “First Discovered” date and the “Mitigated On” date. The components that

depict patch dates use the “Days Since Mitigation” filter to count vulnerabilities that were mitigated within the specified timeframe. The count is based on the number of days between the current date and the “Mitigated On” date. Together, the components in this dashboard can assist security teams with understanding the effectiveness of their patch application and vulnerability remediation efforts.

The manual vulnerability search process works like this. Specific vulnerability data can be found by searching the vulnerability text for keywords, plugin family, severity, or OS CPE strings. For example, perhaps an update was performed on all of the organization's Ubuntu devices to version 21.04. You want to know if any unsupported devices remain in the inventory. From the Findings tab in Tenable Vulnerability Management (or the Analysis tab in Tenable Security Center), and using a filter based on PluginID = 33850, Unsupported Unix Operating Systems, the number of results returned is 78.

A quick review of the details of these assets reveals several different Unix-based Operating systems. At this time we want to focus solely on Ubuntu. By adding a Plugin Output filter of “Ubuntu” we reduce the number of assets to seven.

Another quick review of the details of these assets reveals several different Ubuntu OS versions. However, some of the versions, while unsupported, are still covered by extended security maintenance. As of the time of this writing, Ubuntu version 16.04 support ended on 2021-04-30 (end of maintenance), but had extended security maintenance releases available until 2026-04-30. So we want to focus on patching more vulnerable versions. By changing the Plugin Output filter to “Ubuntu 17” we are returned with one asset.

Looking at the details of this asset we can verify no support for this version has been available since 2018, effectively rendering this asset unpatched for the last five years. In a matter of minutes, using this type of search methodology we have reduced the immediate patching requirement from 78 assets to just a single asset. While the others are also a priority, this one single asset has floated to the top, and can be dealt with immediately, while a plan is developed to patch the remaining assets.

Tenable also publishes Security End of Life (SEoL) plugins to detect and assess products in the SEoL state. SEoL is the state in the Security Maintenance Life Cycle when a product no longer receives security updates. The plugins attempt to abstract various terminologies such as End of Life, Unsupported, End of Support, etc. and provide a clear definition that serves as the basis for SEoL detection plugins. There is a difference between plugins with "Unsupported" in the name and those that are SEoL. SEoL plugins are the evolution of the legacy "Unsupported" plugins. Over time,

all legacy "Unsupported" plugins will be converted to the SEoL detection plugins or enter the deprecation cycle.

For more information on the SEoL plugins, reference this knowledge document.

Vulnerability Assessment/Scanning

Vulnerability assessment is a process that identifies and evaluates network vulnerabilities by constantly scanning and monitoring your organization's entire attack surface for risks. This is the first step in defending your network against vulnerabilities that may threaten your organization.

Authenticated vs. Unauthenticated Scanning

Authenticated (credentialed) and unauthenticated (non-credentialed) scans offer different approaches to vulnerability assessments. They primarily differ in the level of access and permissions granted to the Tenable Nessus scanner. Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results. However, there are benefits to an unauthenticated scan as well. The choice between the two methods depends on the specific goals of the assessment. Often a combination of both will provide the most comprehensive view of a system's vulnerabilities.

The Authentication Summary dashboard for Tenable Vulnerability Management and the Authentication Summary dashboard for Tenable Security Center brings together all the plugins used to verify successful authentication of assets during vulnerability scans, providing security administrators visibility into areas of concern so the appropriate actions can be taken.

Authentication is a process of connecting to a system by providing credentials to gain access. Systems are scanned using different network protocols (SSH, SMB, HTTPS, SNMP, etc.) to gain access to the target asset. For example, logging into a remote host via SSH using a username and password is a method of authentication. Each asset can allow authentication using several protocols. Assets with more than one available authentication protocol (for example, a Windows server running a SQL server) could report both authentication success and failure. Understanding this fact during analysis is key to determining if the system was successfully scanned or not. While in many cases the successful authentication of an asset may seem binary, there are many examples of successfully scanned systems with authentication failures. Tenable recommends system administrators review all of the failures and investigate the services which are enabled on the asset for a complete analysis.

Local checks are required to ensure the scans are complete and accurate. Users enable local checks by providing credentials with elevated privileges, administrative access, or by deploying Tenable Nessus Agents. Tenable Security Center and Tenable Vulnerability Management requires privileged access to provide a comprehensive assessment of risk on an asset. The more access to a system Tenable Security Center and Tenable Vulnerability Management has, the more complete the vulnerability detection.

Authenticated Scan

In the authenticated scan, the Tenable Nessus scanner is provided with a set of valid credentials which are used to access the target systems. The scanner runs with elevated privileges allowing a greater level of access. Authenticated scans provide a more comprehensive and accurate view of a system's vulnerabilities.

Unauthenticated Scan

In the unauthenticated scan, the Nessus scanner does not have valid credentials to access the target system. The scanner can only operate as an external entity and can only attempt to identify vulnerabilities without privileged access. The advantage is that the Nessus scanner mimics the perspective of an external attacker. This could help identify vulnerabilities that could be exploited without authentication. The significant disadvantage, which is typically most associated with a poorly configured scanner or bad credentials, is that a complete picture of the vulnerabilities on the target system will not be identified.

Identifying and Troubleshooting Authentication Problems

Cyber Exposure requires the data collected by the vulnerability scanner to be trusted and verifiable.

Authentication can be defined by connecting to a system and providing credentials in order to gain access to the system. Nessus scans systems by using different network protocols (SSH, SMB, HTTPS, SNMP, etc.) in order to gain access to the remote target asset. For example, logging into a remote host via SSH using a username and password is a method of authentication. Each remote asset can be authenticated using several protocols. Assets with more than one authenticatable protocol (for example, a Windows server running a SQL server) could report both an authentication success and failure. Understanding this fact during analysis is key to understanding if the system was successfully scanned or not. While in many cases the successful authentication of an asset may seem binary, there are many examples of successfully scanned systems with authentication failures. The system administrator should review all the failures and understand the services which are enabled on the asset for a complete analysis.

Local checks are a feature in Tenable Nessus scans, which enable the scanner to perform security checks on the target asset. Different authentication protocols may allow for general checks to be performed locally, but when all possible checks are completed, Tenable Nessus does a more detailed local check. The local check always requires authentication and often requires elevated privileges. Local checks for major operating systems with security advisories numbering in the thousands are often grouped into their own plugin family, but local checks plugins also exist in other families such as Firewalls or Misc.

Enabling local checks is much more complex than authentication and occurs after successful authentication has been established. In order to enable local checks, the following criteria must be satisfied:

- The target device or operating system must be identified.
- Local checks must be available in Tenable Nessus plugins for the identified device or operating system.
- The information needed to enable local checks for that particular device or operating system must be obtained from the remote host.

Except in particular circumstances, such as scanning localhost, remote authentication must first be successful before local checks can be enabled - but the threshold to enable local checks is higher than the threshold for successful authentication.

To ensure the scans report the most complete and accurate information, local checks are a requirement. Users can enable local checks by providing credentials with elevated privileges and/or administrative access or deploying Tenable Nessus Agent. Without elevated access, the ability for Tenable Nessus to successfully identify risk on a system is diminished. The more access to a system Tenable Nessus has, the more complete the risk analysis is.

The following Tenable Nessus plugin IDs are useful in the identification and troubleshooting of scan-related concerns.

Local Authentication

There are a number of useful plugins used to authenticate to the remote host which assist in determining the health of the vulnerability scanning program. These plugins gather the information necessary for local checks, and enable local checks. These plugins can be used to troubleshoot authentication problems. Their output and audit trails provide details of any problems that were encountered. These are:

- 97993 - OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library): Enables local checks over SSH.
- 12634 - Authenticated Check : OS Name and Installed Package Enumeration: Enables local checks over SSH.
- 10394 - Microsoft Windows SMB Login Possible: Enables local checks over SMB.
- 19762 - SNMP settings: Enables local checks over SNMP.
- 73204 - Citrix NetScaler Version Detection: Enables local checks over SSH, SNMP, or NTP.
- 72816 - Palo Alto Networks PAN-OS Version Detection: Enables local checks over HTTP if not already enabled over SSH.
- 57399 - VMware vSphere Installed Patches: This gathers info over HTTPS SOAP API which triggers other plugins to enable local checks.
- 57400 - VMware vSphere Installed VIBs: This gathers info over HTTPS SOAP API which triggers other plugins to enable local checks.

Summarize Specific Auth / Local Checks Issues.

The following plugins provide summaries of particular types of auth / local checks issues that have been reported by other plugins and report the plugins that encountered these issues:

- 102094 - SSH Commands Require Privilege Escalation: Reports commands failed due to lack of privilege escalation or due to failed privilege escalation. Commands reported here may not have prevented local checks from running, but may have caused the plugin associated with each command to fail to produce the expected output. This causes authentication to report as successful, but with insufficient access.
- 110695 - Authentication Success - Local Checks Not Available: Reports local checks were unavailable for the identified device or operating system and includes the report of the plugin that logged the unavailability of local checks.

Successful Login: Windows

- 24269 - WMI Available
- 10394 - Microsoft Windows SMB Login Possible
- 10400 - Microsoft Windows SMB Registry Remotely Accessible
- 10428 - Microsoft Windows SMB Registry Not Fully Accessible Detection
- 57033 - Microsoft Patch Bulletin Feasibility Check
- 20811 - Microsoft Windows Installed Software Enumeration (credentialed check)
- 26921 - Windows Service Pack Out-of-Date
- 34252 - Microsoft Windows Remote Listeners Enumeration (WMI)
- 35703 - SMB Registry : Start the Registry Service during the scan
- 35704 - SMB Registry : Stop the Registry Service after the scan
- 24272 - Network Interfaces Enumeration (WMI)
- 19506 - Nessus Scan Information (Settings)

  > **Note:** For 19506, look for "Credentialed Checks: yes" for a successful scan.

Successful Login: Linux

- 22869 - Software Enumeration (via SSH) (General)
- 12634 - Authenticated Check: OS Name and Installed Package Enumeration (Settings)
- 25221 - Remote listener enumeration (Linux/AIX)

- 33851 - Manually compiled network daemons
- 19506 - Nessus Scan Information (Settings)

> **Note:** For 19506, look for "Credentialed Checks: yes" for a successful scan.

Login Failure/Permission Failure

- 11149 - HTTP login failure (preference): Provides a means for HTTP login info, but also returns login failures when an error happens.
- 21745 - OS Security Patch Assessment Failed: See following note.
- 24786 - Nessus Windows Scan Not Performed with Admin Privileges: This means the account provided for Windows did not have administrator privileges on the scanned host.
- 26917 - Nessus Cannot Access the Windows Registry: This means the target's registry was not available. This is most likely caused by the Remote Registry not set correctly either in the scan policy or on the target.
- 35705 - SMB Registry : Starting the Registry Service during the scan failed: Indicates failure to start remote registry access
- 35706 - SMB Registry : Stopping the Registry Service after the scan failed: Indicates failure to start remote registry access

> **Note:**
>
> More information for plugin 21745 - OS Security Patch Assessment Failed
>
> The plugin 21745 error "unable to create a socket" indicates Nessus was unable to connect to the system. In this case, Nessus was unable to successfully complete the TCP handshake on port 445. This could be for a number of reasons:
>
> - Nessus is unable to connect due to network issues
> - A network or host-based firewall is blocking the connection attempts
> - Due to network latency, a timeout is reached before the connection occurs
> - The user that started the scan does not have permission to scan the given host and/or port
>
> If the user sees this error in plugin 21745 every time authentication fails for a given host, Nessus is having connection issues due to one of the conditions listed above. Nessus users have no

restrictions by default, so this can only happen if an admin explicitly puts any kind of restrictions on users. To determine if this is the case, view the rules file.

To find the rules file:

- Log into Nessus as an administrator.
- Select Configuration > Advanced Settings.
- Scroll down to the rules setting.

Note: If Nessus has too many open sockets during a scan, an error message indicates this problem in nessusd.dump or nessusd.messages.

Summarize Specific Auth / Local Checks Issues

These plugins provide summaries of particular types of auth / local checks issues that have been reported by other plugins and report the plugins that encountered these issues:

- 102094 - SSH Commands Require Privilege Escalation: Reports commands that failed due to lack of privilege escalation or due to failed privilege escalation. Commands reported here may not have prevented local checks from running, but may have caused the plugin associated with each command to fail to produce the expected output. This causes authentication to report as successful, but with insufficient access.
- 110695 - Authentication Success - Local Checks Not Available: Reports local checks were unavailable for the identified device or operating system and includes the report of the plugin that logged the unavailability of local checks.

Summarize Authentication Status

These plugins provide summaries of the overall authentication status for the target. A given target should trigger at least one of these plugins:

- 141118 - Target Credential Status by Authentication Protocol - Valid Credentials Provided: Reports protocols with successful authentication. This plugin reports per protocol, possibly valid credentials can be provided for one protocol and not another. For example, authentication may succeed via SSH but fail via SMB, while no credentials were provided for an available SNMP service.

- 110095 - Target Credential Issues by Authentication Protocol - No Issues Found: Reports protocols with successful authentication and no reported privilege/access issues.
- 110385 - Target Credential Issues by Authentication Protocol - Insufficient Privilege: Reports protocols with successful authentication that also had privilege/access issues logged for the successful credentials.
- 104410 - Target Credential Status by Authentication Protocol - Failure for Provided Credentials: Reports protocols with only authentication failures.
- 110723 - Target Credential Status by Authentication Protocol - No Credentials Provided: Reports protocols that were detected in the scan as available for authentication, but did not have credentials provided for authentication attempts.
- 117885 - Target Credential Issues by Authentication Protocol - Intermittent Authentication Failure: Reports protocols with successful authentication that also had subsequent authentication failures logged for the successful credentials.

Note:

- A given target usually triggers at least one of these unless no services are detected supporting protocols Nessus uses for authentication. Audit trails should indicate this.
- Authentication status is reported per protocol. This means that if there are multiple authentication protocols available on the target with different authentication statuses, possibly both Authentication Success and Authentication Failure can be seen.
- For a given protocol, if both access/privilege problems were encountered and service/authentication problems were encountered, possibly both plugins 110385 and 117885 can be seen.

Summarize Local Checks Status

These plugins provide summaries of overall local checks status for the target. In the case of issues or errors logged by previous plugins, these plugins provide a list of the issues/errors logged along with the reporting plugin and protocol if available.

- 21745 - OS Security Patch Assessment Failed: Reports local checks were not enabled due to an error/failure and lists the details of the errors/failures. Focus on "Local Checks Not Run" rather than the "Authentication Failure" section. While authentication failure is one failure that can cause local checks to be disabled, there are many other types of errors and failures that

prevent enabling local checks.

- 117886 - OS Security Patch Assessment Not Available: Reports local checks were not enabled for an informational reason and lists informational reason details.
- 117887 - OS Security Patch Assessment Available: Reports local checks were enabled. If available, this includes the account and protocol used for local checks.

Additional Resources

An additional list of plugins useful for troubleshooting Tenable Nessus scans can be found here.

Internal Asset Scanning

For more information on getting started with Tenable Nessus, refer to the product documentation located here.

Externally Exposed Asset Scanning

For more information on getting started with Tenable Web App Scanning, refer to the product documentation located here.

Scanning for a Specific Vulnerability

Certain key vulnerabilities may present themselves from time to time. These vulnerabilities, typically called zero-day vulnerabilities, are a flaw or weakness in software, hardware, or firmware unknown to the vendor and does not immediately have a patch available. These vulnerabilities are called zero-day vulnerabilities because once the vulnerability is discovered or exploited, there are zero days to address the issue before potential attacks occur.

These vulnerabilities are highly valuable to attackers because they can launch targeted attacks before a patch is released. Teams must work quickly to analyze their environments and implement a mitigation strategy to minimize the impact of the vulnerability.

To assist organizations with these vulnerabilities, Tenable Research delivers world class exposure intelligence, data science insights, zero day research, and security advisories. Our Security Response Team (SRT) in Tenable Research tracks threat and vulnerability intelligence feeds to make sure our research teams can deliver sensor coverage to our products as quickly as possible. The SRT also works to dig into technical details and author white papers, blogs, and additional communications to ensure stakeholders are fully informed of the latest cyber risks and threats. The SRT provides breakdowns for the latest critical vulnerabilities on the Tenable blog.

When security events rise to the level of taking immediate action, Tenable - leveraging SRT intelligence - notifies customers proactively to provide exposure information, current threat details, and how to use Tenable products and capabilities to accelerate remediation.

Tenable Vulnerability Management and Tenable Security Center contain a Tenable Research Advisories: Urgent Action dashboard.

This dashboard contains indicator style components to highlight any vulnerabilities related to the Tenable Research Advisories where Tenable issues customer guidance that immediate remediation was of paramount importance to all affected organizations. Tenable recommends addressing missing patches as identified in the dashboard components.

Additionally, dashboards exist which focus on specific zero-day vulnerabilities for Tenable Vulnerability Management and Tenable Security Center, such as Heartbleed, Log4shell, and more. Whereas the Tenable Research Advisory dashboard provides an indicator that identifies if the vulnerability is present or has been patched, these focused dashboards provide a higher level of information.

The Tenable Threat Landscape Report (TLR) inspects key aspects of the cybersecurity landscape and describes how organizations can revise their programs to focus on reducing risk. A new TLR is released at the end of each year and highlights the previous 12 months of vulnerabilities and trends.

Dashboards are available for Tenable Security Center and Tenable Vulnerability Management.

The TLR covers:

- Significant vulnerabilities disclosed and exploited throughout the year, including how common cloud misconfigurations can affect even large tech companies.
- The continuous transformation of the ransomware ecosystem and the rise of extortion-only threat groups.
- Ongoing risks, vulnerabilities, and attacks within the software supply chain.
- Tactics used by advanced persistent threat groups to target organizations with cyber espionage as well as financially motivated attacks.
- Breach factors and the challenges in analyzing breach data, given the limited information available and lack of detailed reporting requirements.
- Details of the key vulnerabilities affecting enterprise software.

Using Scan Templates to Scan for a Specific Vulnerability

Scan templates contain granular configuration settings. Team members can use Tenable scan templates to create custom scan configurations for your organization. Then, scans can run based on Tenable scan templates or defined custom configurations' settings. There are three scanner template categories in Tenable Nessus:

Discovery — Tenable recommends using discovery scans to see what assets are on your network and associated information such as IP address, FQDN, operating systems, and open ports if available. With this list of assets, analysts can choose what hosts to target for a specific vulnerability scan.

Vulnerabilities — Tenable recommends using vulnerability scan templates for most of the organization's standard day-to-day scanning needs. Tenable also publishes vulnerability scan templates that allow scanning of the network for a specific vulnerability or group of vulnerabilities. Tenable frequently updates the Tenable Nessus scan template library with templates that detect the latest vulnerabilities of public interest, such as Log4Shell.

Compliance — Tenable recommends using configuration scan templates to check whether host configurations are compliant with various industry standards. Compliance scans are sometimes referred to as configuration scans. For more information about the checks that compliance scans can perform, see Compliance and SCAP Settings.

When a vulnerability is released, organizations immediately begin to ask questions such as:

- Are we vulnerable to this CVE? If so, what assets are vulnerable?
- How do we prioritize our assets?
- How do we validate our patching progress?

Scanning for specific vulnerabilities such as Log4J, can be accomplished using a Scan Template in Tenable Vulnerability Management, within Tenable Security Center (example in the following image) with Scan Policy Templates, or by using a Scan Template in Tenable Nessus.

Web Application Scanning

Tenable Web App Scanning is a dynamic security testing application which crawls a running web application through the frontend to create a site map containing all the pages, links, and forms. Once this site map is created, the data is interrogated to identify any vulnerabilities in the application, custom code, or third-party components.

Web application scanning is of critical importance because users typically access these applications from a browser over the internet. Web applications exist on remote servers or in cloud environments, and data is transmitted over public networks. Web application security is a critical aspect to ensure the confidentiality, integrity, and availability of web applications. Web applications are essential for businesses and individuals, making them lucrative targets for cyber criminals. Attackers focus on exploiting vulnerabilities within web applications to exfiltrate sensitive data, deface web sites, and launch denial of service attacks.

Web applications are commonly susceptible to Cross-Site scripting attacks (XSS), SQL Injections, Cross-Site Request Forgery (CSRF), Insecure Object Reference, and security misconfigurations. Web application security is an ongoing process and requires a multi-layered approach. As threats evolve over time, staying informed about the latest security best practices and keeping applications updated is crucial to protect both the organization and its users from potential harm.

The Open Web Application Security Project (OWASP) is a non-profit organization focused on improving the security of software. Their OWASP Top 10 list highlights the most critical web application security risks, providing guidance on how to prevent and mitigate these vulnerabilities. OWASP has dedicated itself to a release cadence of every three years to respond to the evolving web application security market and address the most common web application vulnerabilities.

Tenable Web App Scanning analyzes web applications and provides deep-dive data on OWASP top 10 vulnerabilities, component vulnerabilities, injections, and in-depth informational details to help organizations identify security concerns in their web applications. The Tenable Web App Scanning landing page for Tenable Vulnerability Management includes some high-level statistics as well as a readout of web application vulnerabilities as they apply to the OWASP Top 10 list.

In addition to the OWASP data, discovered domains are displayed in the Assets view and a new scan can be launched from any discovered domain record. The navigation bar at the top of every view enables users to quickly launch scans by clicking on the Quick Scan button or add a dashboard from the Quick Actions button. Web application assets support AES & ACR scoring, along with Tenable Vulnerability Priority Rating (VPR), which is a dynamic score that helps organizations to prioritize

and strategize remediation based on the immediate risk a vulnerability poses. Updated scan export and new scan import capabilities enables users to import exported scans and see debugging information in web application scan exports to assist with troubleshooting.

Tenable Web App Scanning vulnerability data within Tenable Security Center is available by selecting the Analysis tab, then selecting Web App Scanning to view the web application vulnerability analysis tab.

More information on Web App Scanning can be found in the Cyber Exposure Study: Application Software Security.

As with Tenable Nessus, Tenable Vulnerability Management, and Tenable Security Center, Tenable Web App Scanning contains pre-built templates that assist with common tasks such as:

- Rapid discovery of common cyber-hygiene issues.
- Detection of improperly issued or soon to age out SSL/TLS Certificates.
- Identification of misconfigured web servers.

Summary of Web App Scanning Templates

Scan: The complete set of available checks; all other pre-built templates are a subset of this template other than the API scan.

Overview: A scan that outlines URL paths and builds a site map.

PCI: A special template used as part of the attestation offering Tenable provides for the Payment Card Industry (PCI) security standards. Note: Only submissions to attestation consume PCI licenses, otherwise this operates as a simplified version of the "Scan" template.

SSL/TLS: A health check scan focused on the current state of the web server encryption settings and certificate state such as the remaining time on the certificate.

Config Audit (Tenable Vulnerability Management Only): A compliance audit providing detection of externally viewable web server settings, which external audit providers commonly review to evaluate the health of a security program.

API Scan: A special template requiring additional configuration to describe the application programming interface (API) so the scanner can successfully detect relevant vulnerabilities. This includes some of the same tests as the "Scan" template, but adds others unique to API endpoints.

Quick Scan: A simplified version of the "Scan" template with several of the active tests removed to lower the impact and speed up the scan.

Log4Shell: A scan to specifically detect Apache Log4J (CVE-2021-44228).

Vulnerability Remediation

Timely and effective remediation remains the Achilles' heel for too many organizations. Even if security teams identify a concise list of prioritized CVEs, they must work closely with their IT counterparts to address those issues, providing detailed information about how to remediate each vulnerability and why it's a priority. Without adequate teamwork, the security program is not nearly as effective.

Remediation also involves indirect costs, whether that's IT Operations or Information Security team's time or the cost of taking down a business-critical system to install and test a patch. The teams are required to efficiently allocate resources where they can have the greatest impact for the least amount of effort.

Tracking and Reporting SLA Progress

Once the highest priority vulnerabilities are identified, operations team needs to take the appropriate action to effectively manage the risk. For each vulnerability, there are three response options — remediate, mitigate, or accept. Which action is chosen for each should be in line with what was previously determined during the initial discovery phase, as you developed a comprehensive understanding of the environment. But to be sure we're clear on our terminology, here's how we define each of them:

Remediate

Oftentimes, remediation is used interchangeably with patching. And in some cases, patching may be all that's required. Something important to note is that typically, applying a patch is just one part of what's required to remediate a vulnerability. The asset may also require removal or rebuilding the operating system, specific software components may need to be upgraded, or there could be a configuration error that needs to be corrected. Once the vulnerability is verified to have been fully remediated, the amount of risk associated with the vulnerability is fully removed from the environment.

Mitigate

Mitigation employs other technologies to reduce the risk of a given vulnerability. This is different from remediation because with mitigation nothing has really been done to actually fix the vulnerability itself. Instead, organizations are accounting for other mitigating factors that neutralize some or all of the risk posed by the vulnerability. For example, organizations may have firewall rules in place that effectively block an exploit from accessing sensitive data. To account for this mitigating factor, organizations would reduce the severity of the vulnerability accordingly.

Accept

Risk acceptance is consciously deciding not to take any action at all. This may be done for a variety of reasons. For example, during the discovery phase, management may have determined some assets are so business-critical they can't afford to take them down for maintenance unless the vulnerability is also business-critical. In other cases, the cost of the fix may be greater than the cost associated with a successful exploit. Regardless of the reason, when organizations choose to accept risk, the VM platform may allow you to remove the risk score from reports or set the score to "0." However, organizations need to understand that while the vulnerability may no longer be immediately visible, the actual risk still remains in your environment.

> **Note:** If you're in an industry subject to regulatory compliance, don't be tempted to develop an assessment plan around passing audits. Limiting assessments to assets that are within audit scope often causes other business-critical systems to be ignored. Remember passing an audit doesn't mean you're secure.

These actions should align with the organizational plans established during the discovery phase of the risk-based VM lifecycle when the business environment was mapped, along with IT policies, and procedures.

How Tenable Lumin Can Help

Tenable Lumin summarizes key assessment maturity metrics to help improve assessment capabilities and security responsiveness. Tenable Lumin provides detailed analysis into asset scan distribution, frequency, and vulnerability age to strengthen program effectiveness and focus on process maturity. Interactive widgets allow analysts to drill into assessment maturity data to investigate the security posture of underlying assets. Tenable Lumin measures remediation responsiveness, remediation coverage, and provides the proper context for an organization's process risk mitigation efforts.

The metrics provided by Remediation Maturity scores allow organizations to pinpoint the specific strengths and weaknesses of their remediation efforts. They can use this information to better understand their processes and modify them accordingly - either by changing those processes and/or making further investments.

Remediation maturity metrics include:

- Remediation Maturity Grade (A-F) for Org and Business Contexts
- Remediation Maturity Trending (Organizations vs Industry vs Population)
- Remediation Responsiveness Grade → Remediation Time Since -- Recovery and Remediation Time Since Vulnerability Publication

Tenable Lumin provides security teams with a list of the top recommended actions that reduce the most cyber exposure, to translate business decisions on risk appetite to technical guidance for teams to action. For additional information, teams can drill down into specific vulnerabilities or assets for business and risk context to enable more effective remediation.

Use the Tenable Lumin dashboard to understand your CES and access details pages.

- (1) Cyber Exposure Score widget — How does your overall risk compare to other Tenable customers in your Salesforce industry and the larger population?
- (2) Cyber Exposure Distribution Trend widget — How has the overall risk for your entire organization changed over time?
- (3) Assessment Maturity widget — How frequently and thoroughly are you scanning your assets?

- (4) Remediation Maturity widget — How quickly and thoroughly are you remediating vulnerabilities on your assets?
- (5) Cyber Exposure Alerts widget — What important cyber security alerts you should be aware of?
- (6) Actions to Reduce CES widget — What would the impact be if you addressed these recommended actions?
- (7) Mitigations widget — What endpoint protection agents are running on your assets?
- (8) Cyber Exposure Score by Business Context/Tag widget — How do assets with different tags (unique business context) compare?

By drilling down into these widgets, organizations can get a detailed picture of their remediation progress and standing. For example, by drilling down into the (4) Remediation Maturity widget presents a wealth of remediation information, from a grade standing on remediation progress against other peer organizations, to recommended actions and remediation timeframes.

By drilling down into these widgets, organizations can get a detailed picture of their remediation progress and standing. For example, by drilling down into the (4) Remediation Maturity widget presents a wealth of remediation information, from a grade standing on remediation progress against other peer organizations, to recommended actions and remediation timeframes...

...and the (2) Remediation Coverage Grade, which measures the percentage of vulnerabilities remediated on your assets, organized by VPR category.

More information on getting started with Tenable Lumin can be found here.

How Tenable Vulnerability Management and Tenable Security Center Can Help

Tenable Vulnerability Management contains the Fundamental Cyber Hygiene Report Card dashboard, which can be reviewed here. As vulnerabilities are identified, remediation must be prioritized and tracked in accordance with organizational goals and Service Level Agreements (SLAs). Reviewing remediated vulnerabilities and the remediation timeframe provides valuable information to the organization on the effectiveness of the risk remediation program. Three widgets focus on this area to assist organizations:

Vulnerability Age: Managing SLAs: This widget provides a view of vulnerabilities based on severity and age. The columns display counts of vulnerabilities that have been published within the specified time period and are present in the organization. The rows display the severity level of the vulnerability. Organizations can use this information to determine their compliance with organizational policy and Service Level Agreements (SLAs). For example, if an organization has a SLA that states Critical/High vulnerabilities must be patched within 45 days, any data displayed in the first three columns and two rows indicates non-compliance with the SLA. Vulnerability age is determined from the time the vulnerability was published.

Outstanding Remediations - Time Since Patch Publication: This widget displays the total count of missing patches across the environment. The matrix is composed of five columns. The first column provides a count of the vulnerabilities that are exploitable and the last four columns provide counts of vulnerabilities based on severity levels. Each row filters the vulnerabilities based on the patch publication date of less than 30 days ago, 31-90 days, 91-180 days, and greater than 181 days.

Outstanding Microsoft Remediations - Time since Patch Publication: This widget displays the total count of missing patches related to Microsoft Security Bulletins using the Windows: Microsoft Bulletins and Windows plugin families. The matrix is composed of five columns. The first column provides a count of the vulnerabilities that are exploitable and the last four columns provide counts of vulnerabilities based on severity levels. Each row filters the vulnerabilities based on the patch publication date of less than 30 days ago, 31-90 days, 91-180 days, and greater than 181 days.

Drilling down into the cells present similar details, with the exception of the filters that are used for each cell in each widget. Some of the important details to view are:

Tenable Security Center provides a Getting Started with Tenable.sc Using SLA's dashboard, more details can be found here.

This dashboard is commonly used by the sales team at Tenable to help coach organizations to meet SLAs. The components in this dashboard are grouped in 3-series, which provide a CISO and Risk Manager with a starting point for SLA analysis.

The first few rows provide a detailed analysis on SLAs for vulnerabilities based on CVSS and VPR. Traditionally many SLAs are based on Microsoft's Patch Tuesday and provide organizations a period of 30 days to apply newly released patches. While this is common, with Tenable's VPR score the Risk Managers can now better understand the risk to an environment when a vulnerability is detected.

The second grouping provides overall asset detection and inventory metrics. Starting in the upper-left corner, the number of systems with completed audit checks is displayed, down to authentication statuses. The trend line on the far right provides a history of asset counts via passive and active detections.

The remaining components provide examples of how analysts can focus on specific vulnerabilities. For example, the Spectre/Meltdown vulnerabilities are detected using the CVE related to the vulnerability. Also, the most critical hosts based on VPR score are also provided. There are several different views based on different tools. For example, the Remediation Summary tools provide a series of patches available to mitigate the most risk. There are two examples, one based on the VPR score and the other based on CVSS severity. The organization can compare the two results to better understand the necessary actions needed to achieve the most risk mitigation.

All of these components together provide a starting point, which is useful throughout the Tenable customer base. Organizations are encouraged to install this dashboard and set the focus to different repositories, dynamic assets, or static assets allowing for risk to be analyzed separately. Administrators can also use this dashboard as a starting point to create their own dashboard by installing the dashboard, setting focus, and then copying the components to a common dashboard. Overall this dashboard is a great place to start when upstanding the SLA compliance.

In Closing

Now that you've completed measuring your mitigation strategy against the organization's SLAs, you're able to determine the effectiveness of the organization's risk-based vulnerability management program, including what's working well and where there are areas for improvement. This is called Continuous Improvement. This knowledge helps you communicate the value of your security program to senior management and other key stakeholders so you can effectively build their confidence in your capabilities, request additional resources, and manage expectations when high-profile cyber attacks draw media attention.

With a specific, quantifiable understanding of how the RBVM program has performed, you'll also know exactly what adjustments to make in order to optimize your team's effectiveness and efficiency as you continue to evolve your VM practices to align with a risk-based strategy.

Compliance References

CSF v1.1 References

ID.RA-1

ID.RA-5

PR.IP-12

NIST Special Publication 800-53 Revision 5

- RA-5: Vulnerability Monitoring and Scanning
- RA-7: Risk Response
- SI-2: Flaw Remediation
- SI-2(2): Automated Flaw Remediation Status

NIST Special Publication 800-53 Revision 4

- RA-5: Vulnerability Scanning
- SI-2: Flaw Remediation
- SI-2(2): Automated Flaw Remediation Status

NIST Special Publication 800-171 Revision 2

- 3.11.2: Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.