Tenable Cyber Exposure Study – System Hardening and Log Management

Last Revised: April 09, 2025

Table of Contents

System Hardening and Log Management Executive Overview

In today's climate, new vulnerabilities emerge as critical and exploitable but avoidable threats to enterprise assets and software. When deploying and maintaining enterprise assets and software being proactive is important and, as the configurations are normally geared towards ease-of-deployment and ease-of-use the user needs to ensure security is still the main focus.

By default, a lot of modern infrastructure is not in the most secure configuration possible. The default configuration of assets and software leads to avenues of attack for threat actors and should be rectified. Some areas of enterprise software deployments where actions can be taken to seal up configuration holes include: Services, Apps, Protocols; Account Management; Resource Control; Network Monitoring, and Log Collection. Organizations who approach cyber security proactively, leverage established frameworks and guidelines such as Critical Security Controls version 8 (CIS CSCv8) established by the Center of Internet Security. This study walks the reader through the different topics of System Hardening and Log Management. The study also shows how Tenable can help verify and track compliance. Lastly, the study describes how the user can use Tenable to visualize their compliance data.

This Cyber Exposure Study provides guidance through the following subjects:

- Introduction to Searching
    - This section breaks down and introduces searching and identifying keywords and patterns to use after a compliance policy scan. Audit files are also broken down to lay out what can be used to focus the queries in the Tenable Vulnerability Management and Security Center.
- System Hardening
    - Involving the hardening of enterprise assets and software similar to the CIS Control 4: Secure Configuration of Enterprise Assets and Software describes how an asset should be configured. Tenable can help security teams understand and track compliance with secure configuration standards.
- Log Collection and Management

- Log Collection and Management reinforces the secure configuration by ensuring audit logs and system logs are properly set up and enabled. Tenable is able to allow the user to verify certain logging configuration settings with the use of compliance scanning.

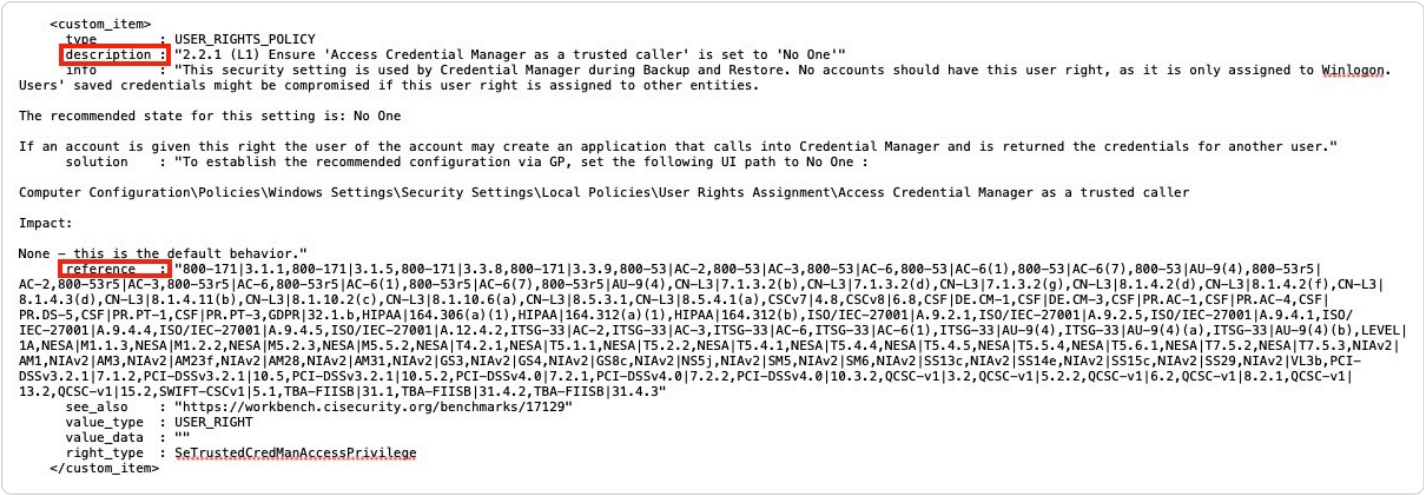
- Network Hardening and Monitoring
  - The CIS Control 12: Network Infrastructure Management describes how network devices should be established, managed, and implemented to thwart potential attackers.
- Widget/Component Creation
  - After understanding how to query results from compliance scans, creating widgets in Tenable Vulnerability Management or components in Tenable Security Center can assist security team in visualizing the data. These widgets/components can be used in both Dashboards and reports.

Search Overview

When scanning for assets to track compliance efforts, Tenable Audit files are used to instruct the scan of specific configuration, file permission, and access control tests to be performed. Knowing the source is important before looking at the audit results. Being familiar with the file structure, key data fields, and how the fields translate into filters in Tenable Vulnerability Management and Tenable Security Center can assist the user in fine-tuning their focus, and query the results that are needed from the audit scan.

Audit Files:

Audit files that can be used in the scans are formatted like an XML. This formatting allows the file to be pretty readable and provides the ability to grep through the audit file to identify key fields that will help determine what the benchmark or specific test is about. Within the audit files there are many elements called <item> or <custom_item>. These items delineate the various checks or tests involved in the audit benchmark. Within these “items” there are two main elements that should be a focus: “description” and “reference."



```
    <custom_item>
      type        : USER_RIGHTS_POLICY
      description : "2.2.1 (L1) Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'"
      info        : "This security setting is used by Credential Manager during Backup and Restore. No accounts should have this user right, as it is only assigned to Winlogon.
Users' saved credentials might be compromised if this user right is assigned to other entities.

The recommended state for this setting is: No One

If an account is given this right the user of the account may create an application that calls into Credential Manager and is returned the credentials for another user."
      solution    : "To establish the recommended configuration via GP, set the following UI path to No One :

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller

Impact:

None - this is the default behavior."
      reference   : "800-171|3.1.1,800-171|3.1.5,800-171|3.3.8,800-171|3.3.9,800-53|AC-2,800-53|AC-3,800-53|AC-6,800-53|AC-6(1),800-53|AC-6(7),800-53|AU-9(4),800-53r5|
AC-2,800-53r5|AC-3,800-53r5|AC-6,800-53r5|AC-6(1),800-53r5|AC-6(7),800-53r5|AU-9(4),CN-L3|7.1.3.2(b),CN-L3|7.1.3.2(d),CN-L3|7.1.3.2(g),CN-L3|8.1.4.2(d),CN-L3|8.1.4.2(f),CN-L3|
8.1.4.3(d),CN-L3|8.1.4.11(b),CN-L3|8.1.10.2(c),CN-L3|8.1.10.6(a),CN-L3|8.5.3.1,CN-L3|8.5.4.1(a),CSCv7|4.8,CSCv8|6.8,CSF|DE.CM-1,CSF|DE.CM-3,CSF|PR.AC-1,CSF|PR.AC-4,CSF|
PR.DS-5,CSF|PR.PT-1,CSF|PR.PT-3,GDPR|32.1.b,HIPAA|164.306(a)(1),HIPAA|164.312(a)(1),HIPAA|164.312(b),ISO/IEC-27001|A.9.2.1,ISO/IEC-27001|A.9.2.5,ISO/IEC-27001|A.9.4.1,ISO/
IEC-27001|A.9.4.4,ISO/IEC-27001|A.9.4.5,ISO/IEC-27001|A.12.4.2,ITSG-33|AC-2,ITSG-33|AC-3,ITSG-33|AC-6,ITSG-33|AC-6(1),ITSG-33|AU-9(4),ITSG-33|AU-9(4)(a),ITSG-33|AU-9(4)(b),LEVEL|
1A,NESA|M1.1.3,NESA|M1.2.2,NESA|M5.2.3,NESA|M5.5.2,NESA|T4.2.1,NESA|T5.1.1,NESA|T5.2.2,NESA|T5.4.1,NESA|T5.4.4,NESA|T5.4.5,NESA|T5.5.4,NESA|T5.6.1,NESA|T7.5.2,NESA|T7.5.3,NIAv2|
AM1,NIAv2|AM3,NIAv2|AM23f,NIAv2|AM28,NIAv2|AM31,NIAv2|GS3,NIAv2|GS4,NIAv2|GS8c,NIAv2|NS5j,NIAv2|SM5,NIAv2|SM6,NIAv2|SS13c,NIAv2|SS14e,NIAv2|SS15c,NIAv2|SS29,NIAv2|VL3b,PCI-
DSSv3.2.1|7.1.2,PCI-DSSv3.2.1|10.5,PCI-DSSv3.2.1|10.5.2,PCI-DSSv4.0|7.2.1,PCI-DSSv4.0|7.2.2,PCI-DSSv4.0|10.3.2,QCSC-v1|3.2,QCSC-v1|5.2.2,QCSC-v1|6.2,QCSC-v1|8.2.1,QCSC-v1|
13.2,QCSC-v1|15.2,SWIFT-CSCv1|5.1,TBA-FIISB|31.1,TBA-FIISB|31.4.2,TBA-FIISB|31.4.3"
      see_also    : "https://workbench.cisecurity.org/benchmarks/17129"
      value_type  : USER_RIGHT
      value_data  : ""
      right_type  : SeTrustedCredManAccessPrivilege
    </custom_item>
```

The “description” field within the “items" element is the name of the actual audit check that will be performed. Within Tenable Vulnerability Management these checks can be searched using the filter “Audit Check Name”, and within Tenable Security Center the description field becomes the plugin name: therefore, the plugin name filter would be used.

The “reference” field is the next important field that is used for compliance-based analysis. The reference field is used to map a variety of compliance frameworks and the associated control identifiers to a specific audit check. After the audit file has been used in a scan, the reference field

in the audit file can be searched for in Tenable Vulnerability Management by using the Compliance Framework Filter and the Compliance Control Filter, while in Tenable Security Center the user would need to use the Cross Reference filter.

This study takes a closer look at searching for compliance goals by querying audit checks and cross-references using Tenable Vulnerability Management and Tenable Security Center. Before querying the results in Tenable Vulnerability Management or Tenable Security Center the user may be wondering what the audit file tests or what the audit file attempts to achieve. A user is able to search through the audit files used in the scans to find reference information, or even audit check names, for the related audit checks.

In **macOS and Linux systems** a simple "grep" command can be used to quickly identify which audit checks may be of interest.

```
TENA000878:auditFile20May cnavas$ grep -E '.*description.*updates.*' CIS_Microsoft_Windows_10_Stand-alone_v3.0.0_L1.audit
      description : "18.10.65.3 (L1) Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'"
      description : "18.10.92.1.1 (L1) Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'"
      description : "18.10.92.2.3 (L1) Ensure 'Remove access to 'Pause updates' feature' is set to 'Enabled'"
```

In Windows, a user can use the "type" command along with the "findstr" in the command prompt to look through audit files and find desired audit checks.

```
C:\Users\Administrator\Downloads>type CIS_Microsoft_Windows_Server_2019_Benchmark_v2.0.0_L1_DC.audit | findstr updates
```

This search is also possible in powershell. One quick way is using the "Get-Content" and "Select-String" commands.

```
PS C:\Users\Administrator\Downloads> Get-Content .\CIS_Microsoft_Windows_Server_2019_Benchmark_v2.0.0_L1_DC.audit | Select-String "updates"
```

For a more detailed breakdown of the structure of audit files go to refer to the Host Audit Data cyber exposure study.

System Hardening

Services and Apps

Setting up secure configurations of assets and software could include removing or disabling unnecessary services, apps, and/or protocols. Common protocols that may not be used and should be disabled could be: Telnet, FTP, SMTP, etc. The actual services needed depend on the needs and uses of the user of the asset, which also need to be blueprinted. When possible, removing an unnecessary service is preferable to disabling since disabling still allows a malicious user to re-enable the service/protocol and exploit the system further.

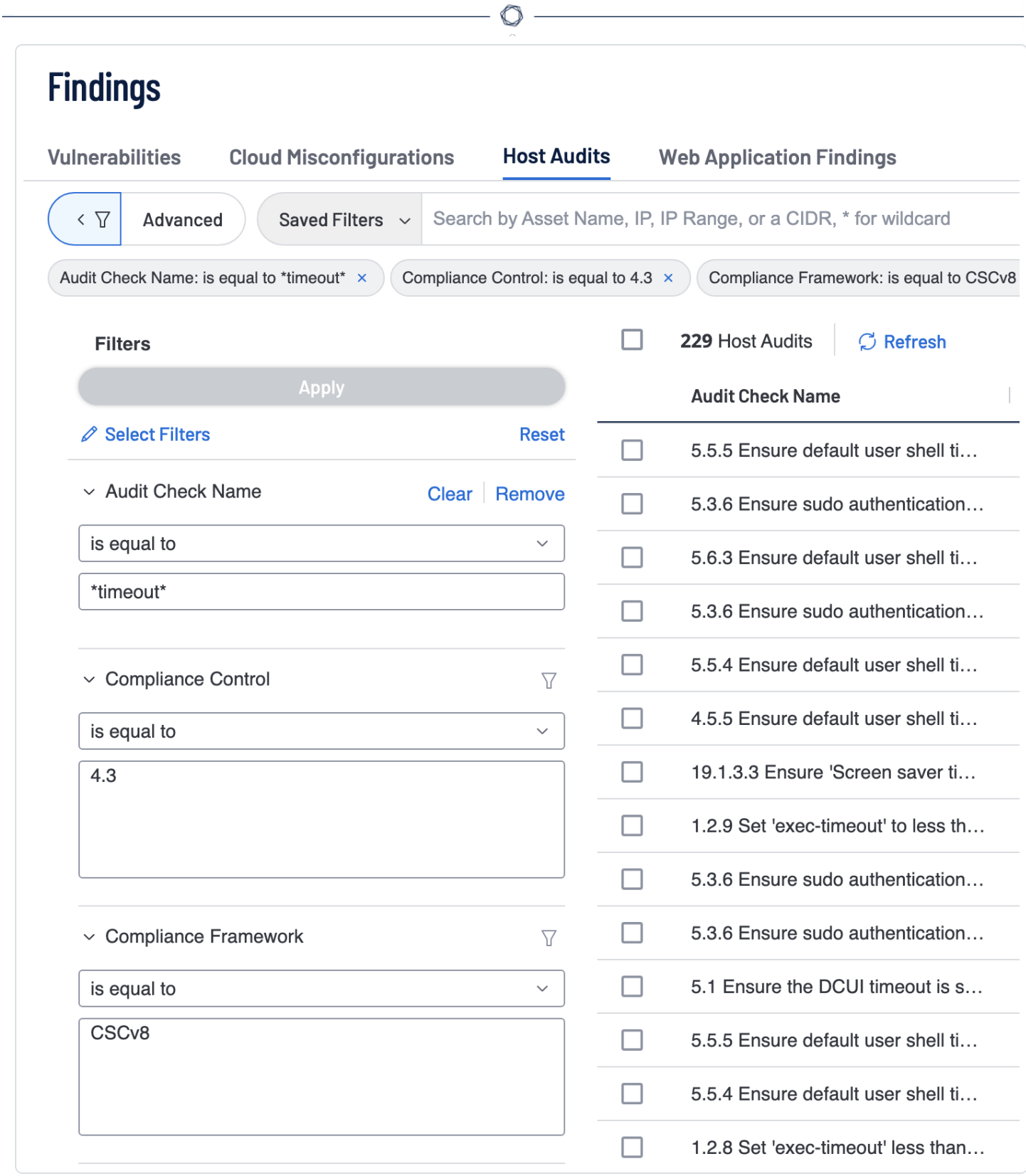
Enterprises can also start to secure their configurations by looking at publicly developed, vetted, and supported Security Benchmarks, security guides, or checklists; some examples include the CIS Critical Security Controls, NIST's National Checklist Program, and SANS Security Policy Templates.

Search Examples

While the detection plugins are useful, they do not provide the complete solution. Credentialed compliance scanning is the correct solution for finding possible services, or clients that shouldn't be there. For example, CIS Control version 8 4.8 states "Uninstall or Disable unnecessary services on enterprise assets and software", this means when using CIS audits while scanning, there are audit checks that specifically look and check if there are services, or clients that should be disabled/uninstalled based on recommended secure configurations.

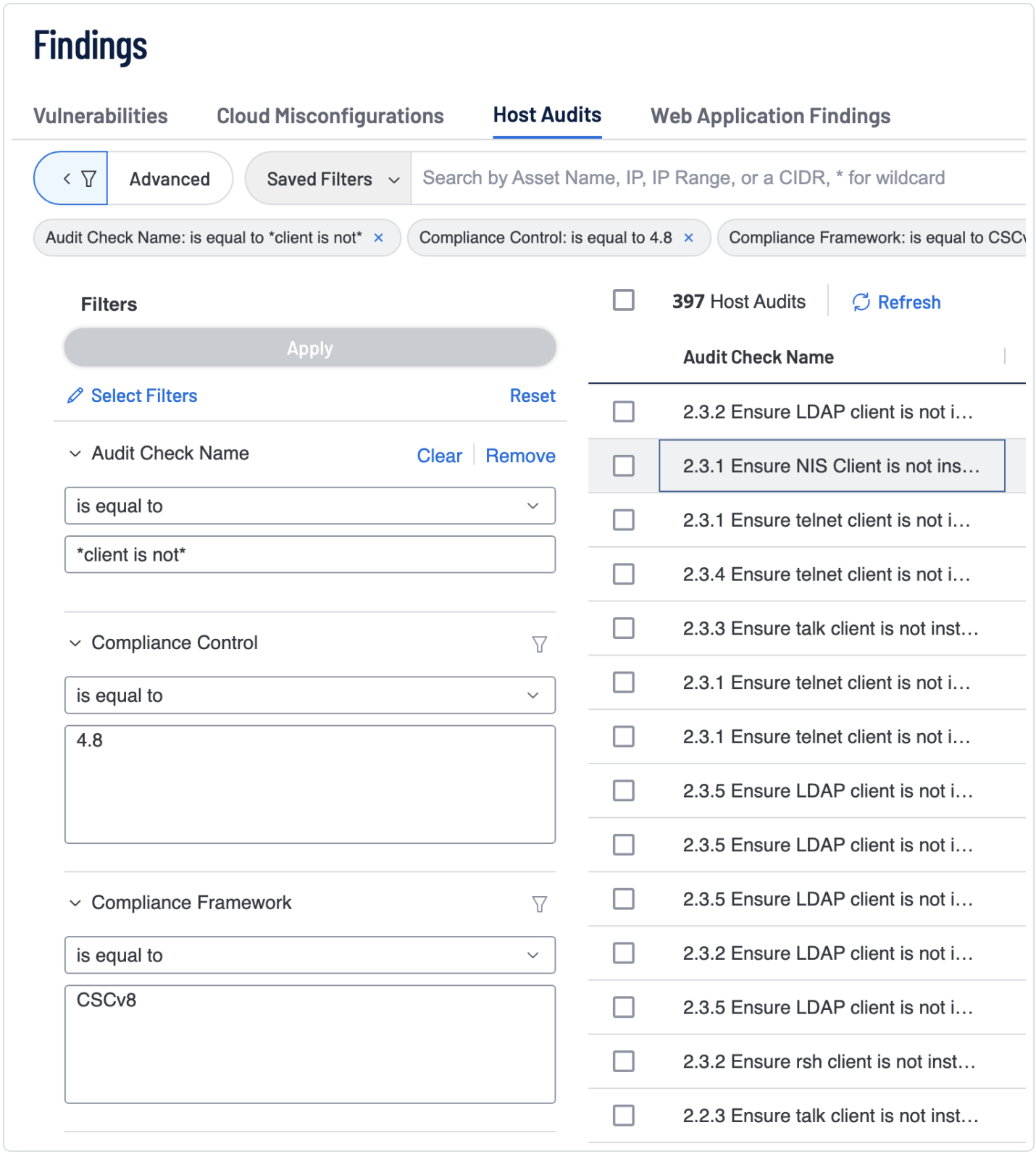
Tenable Vulnerability Management

In Tenable Vulnerability Management these audit checks can be found using the Audit Check Name filter and searching for either *service is not* or *client is not*. An example of an audit check that would be returned with this query would be "2.3.1 Ensure NIS Client is not installed".

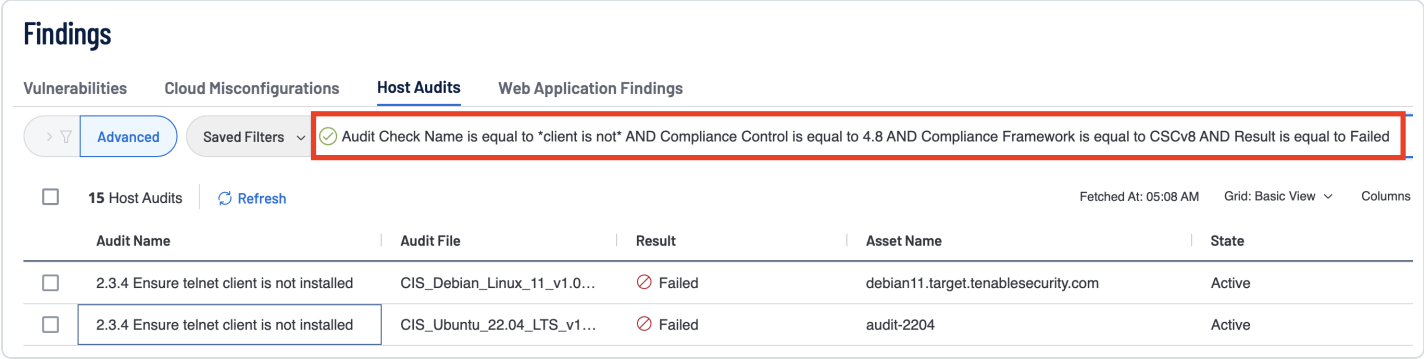


Another way to efficiently filter the audit results in Tenable Vulnerability Management is by using the Compliance Control Filter. For example, in this case we can search for Compliance Control is

equal to 4.8 to display audit checks that relate to CIS 4.8. To further filter out the previous query the **Compliance Framework filter** can also be used.



Using a combination of the filters can allow the search to be more precise, as some compliance frameworks may have similar numbering, or newer versions of a framework may have renumbered some of the checks. In the previous examples it's apparent that using the combinations of filters reduced the number of results that came back: 397 Host Audits from the original 533 when only using the Audit Check Name filter. This reduction of Host Audits displays the usefulness of using more than one filter to enhance the search.



The previous query can be replicated exactly by selecting the "Advanced button" within the Host Audits section of the findings page and inputting any of the following queries:

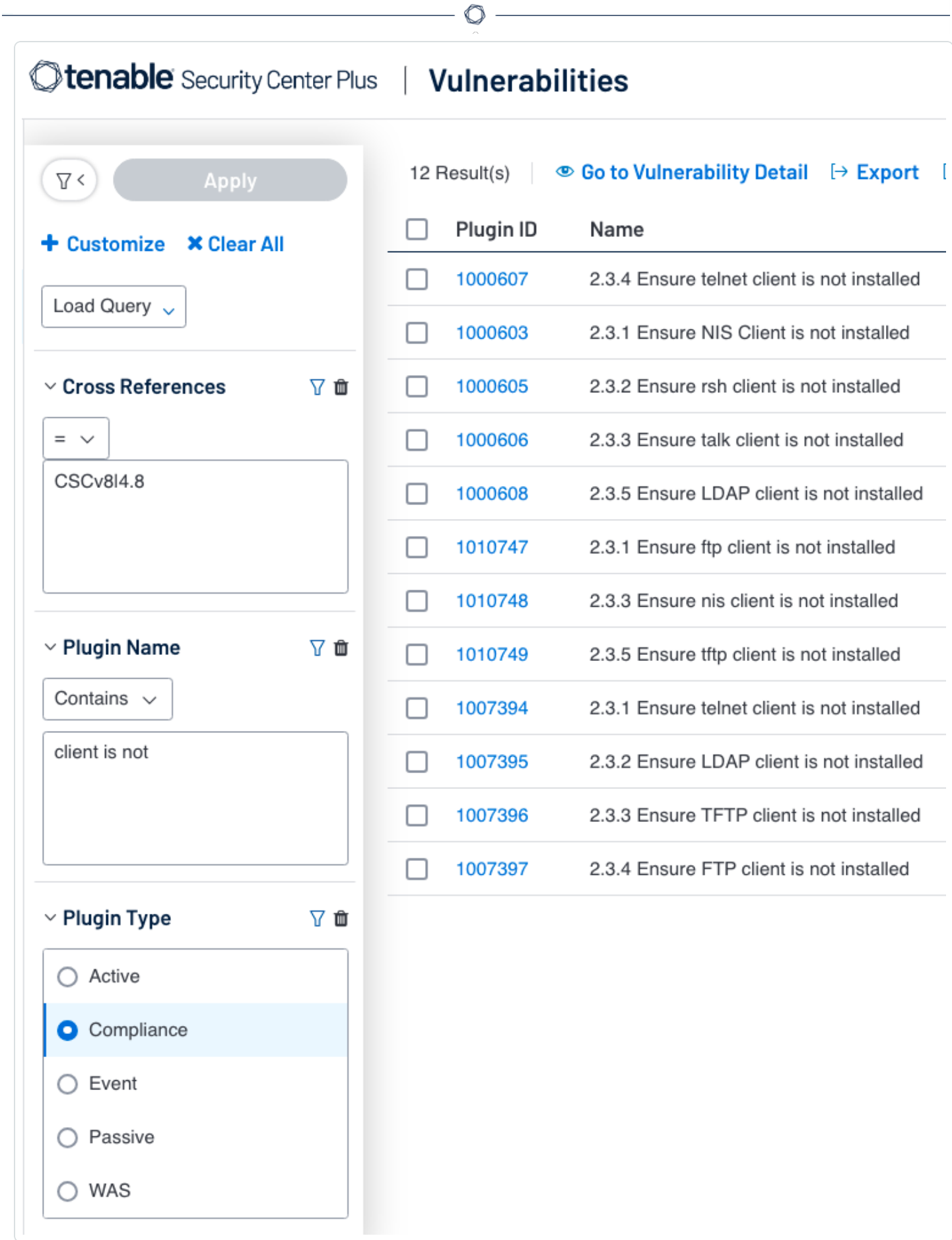
- Audit Check Name is equal to *client is not* AND Compliance Control is equal to 4.8 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *service is not* AND Compliance Control is equal to 4 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed

Tenable Security Center

In Tenable Security Center, the Cross Reference filter takes the place of the Compliance Framework filter and Compliance Control filter which are used in Tenable Vulnerability Management. Though, much like within Tenable Vulnerability Management, using other filters to enhance the search is advisable. Instead of an Audit Check Name Filter, in Tenable Security Center a user can use the combination of Plugin Type Filter set to Compliance plugins, and Plugin Name filter to look for the audit check. Tenable Security Center allows a regex match to be used for the plugin name or just a simple *contains* search. A possible query for Plugin Name contains "client is not" along with Plugin Type set to Compliance, and this query would result in audit checks run. Pair the previous two filters with the **Cross Reference Filter**.

In Tenable Security Center the Cross Reference filter allows the query to filter on audit checks that relate to a specific framework and specific controls within those frameworks. For CIS Control 4 the

user can utilize the Cross Reference to equal “CSCv8|4.*” (shown in the above image). The Cross Reference filter expects the desired compliance framework followed by the control and separated by a pipe (|). A valid query could also be “CSCv8|*” if a specific control isn’t needed and all audit checks related to the framework are desired.


tenable Security Center Plus | Vulnerabilities
Apply
+ Customize
✖ Clear All
Load Query
Cross References
=
CSCv8l4.8
Plugin Name
Contains
client is not
Plugin Type
Active
Compliance
Event
Passive
WAS
12 Result(s)
Go to Vulnerability Detail
Export
Plugin ID
Name
1000607 2.3.4 Ensure telnet client is not installed
1000603 2.3.1 Ensure NIS Client is not installed
1000605 2.3.2 Ensure rsh client is not installed
1000606 2.3.3 Ensure talk client is not installed
1000608 2.3.5 Ensure LDAP client is not installed
1010747 2.3.1 Ensure ftp client is not installed
1010748 2.3.3 Ensure nis client is not installed
1010749 2.3.5 Ensure tftp client is not installed
1007394 2.3.1 Ensure telnet client is not installed
1007395 2.3.2 Ensure LDAP client is not installed
1007396 2.3.3 Ensure TFTP client is not installed
1007397 2.3.4 Ensure FTP client is not installed

Related Controls: 800-171 3.4.2, 800-53r5 CM-7, CSCv7 9.2/CSCv8 4.8, CSF PR.IP-1,PR.PT-3, ISO-27001 A.6.2.2,A.10.1.1,A.13.2.3

Keyword	Common Windows Audit Name	Common Unix Audit Name
remote	"5.24 Ensure 'Remote Procedure Call (RPC) Locator (RpcLocator)' is set to 'Disabled'"	"3.5.6 Remote daemon lockdown - rlogind"
port	"18.10.57.3.3.1 Ensure 'Do not allow COM port redirection' is set to 'Enabled'"	"Loopback on Port 25"
Server	"18.4.4 Ensure 'Configure SMB v1 server' is set to 'Disabled'"	"2.2.4 Ensure DHCP Server is not installed - isc-dhcp-server"
Service	"5.11 Ensure 'Microsoft FTP Service (FTPSVC)' is set to 'Disabled' or 'Not Installed'"	"rsyncd.socket rsyncd.service active"
Is installed	N/A	"telnet-server is installed"
disabled	"18.5.19.2.1 Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)')"	"3.3.3 Ensure IPv6 is disabled"

Note: When searching a keyword in Tenable Security Center (Plugin Name filter), the plugin type compliance filter should be used along with a cross reference filter to eliminate any false positives in the query.

In Tenable Security Center the Cross Reference filter allows the query to filter on audit checks that relate to a specific framework and specific controls within those frameworks. For CIS Control 4 the user can utilize the Cross Reference to equal "CSCv8|4.*" (shown in the above image). The Cross Reference filter expects the desired compliance framework followed by the control and separated by a pipe (|). A valid query could also be "CSCv8|*" if a specific control isn't needed and all audit checks related to the framework are desired.

State	Tenable Security Center Severity	Tenable Vulnerability Management State	Descriptions

PASSED	Informational	Passed	The audit check was within the tested parameters.
FAILED	High	Failed	The audit check was not within the tested parameters.
ERROR	Medium	Error	The audit check is not supported on the asset.
WARNING	Medium	Warning	The audit check was successful, however compliance cannot be determined and needs to be reviewed manually.

Updates and Patches

Ensuring enterprise assets and software are up to date by having the latest security patches is also imperative when achieving a secure configuration. Security updates and patches may appear to be tedious at times, but with the ever-evolving cyber landscape new exploits are discovered and need to be patched up. Ensuring settings like automatic updates or configuring a regular schedule for system updates can give the user confidence the system won't be at risk from a known exploit. Along with regular updates, using regularly maintained and supported operating systems is important. When some operating systems become End-Of-Life, no more security updates are pushed out, therefore, any new exploits after the fact become harder to mitigate. Tenable can assist the user establish a baseline and track compliance by querying results from credentialed scans.

Search Examples

Verifying systems are patched can be done by searching for audit names including keywords like "patches", "automatic updates" or a combination of "updates" and "security". Queries using those keywords result in audit check names involving being assured the latest security patches are installed.

The following table provides common keywords that can be used to query audit results in both Tenable Security Center and Tenable Vulnerability Management.

Keyword	Common Windows Audit Name	Common Unix Audit Name

Patches	N/A	"6.5 Ensure Applicable Patches Are Applied"
Updates + security	"1.1 Ensure Latest SQL Server Cumulative and Security Updates are Installed"	"1.8 Ensure updates, patches, and additional security software are installed"
Automatic Updates	"18.10.92.2.1 (L1) Ensure 'Configure Automatic Updates' is set to 'Enabled'"	N/A

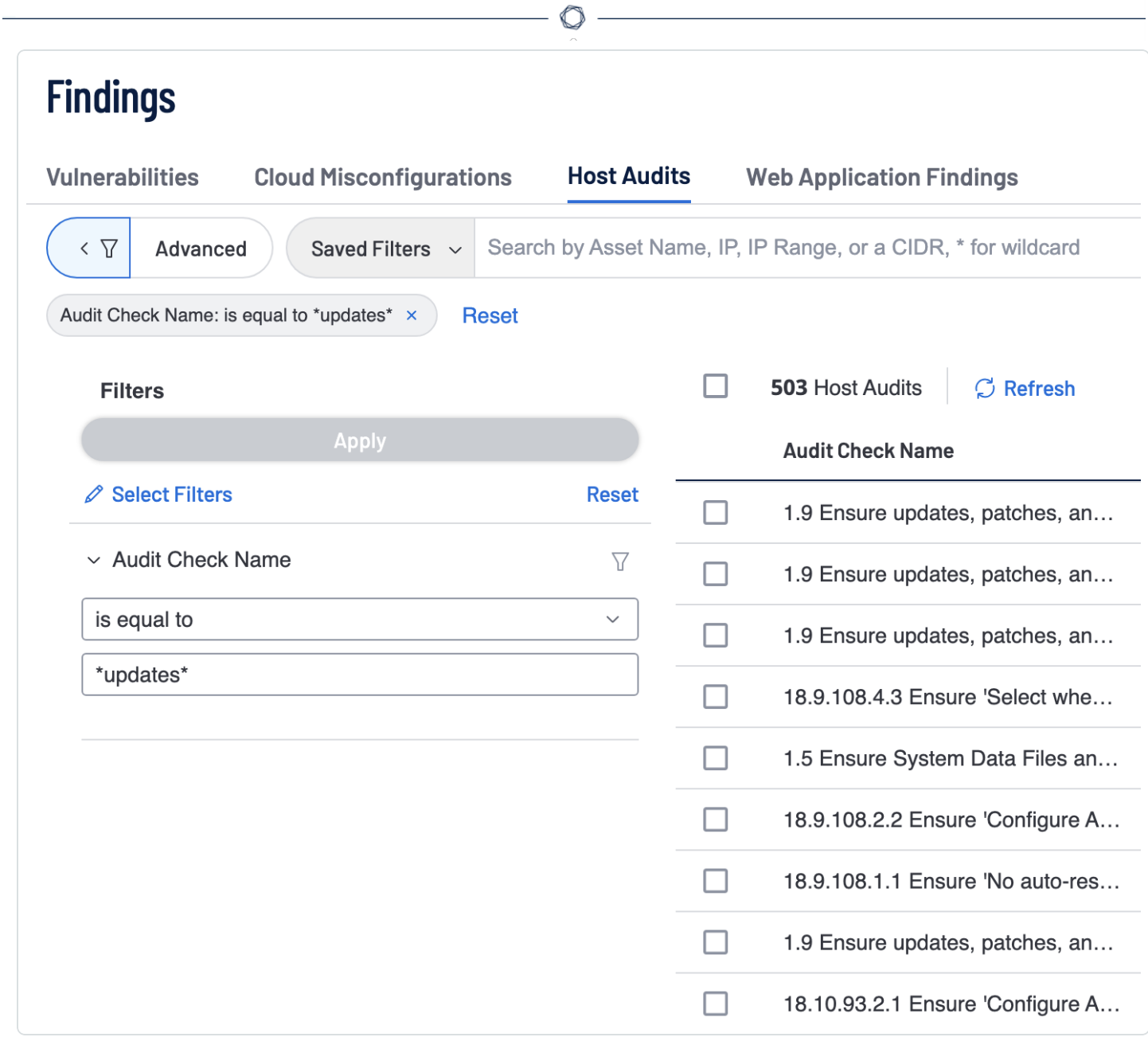
Note: When searching a keyword in Tenable Security Center (Plugin Name filter), the plugin type compliance filter should be used along with a cross reference filter to eliminate any false positives in the query.

To further focus on relevant audit results we can hone in on related controls. These related controls reside in the reference information element of each item in the audit file and can be queried in Tenable Security Center by using the cross-reference filter and in Tenable Vulnerability Management by using the Compliance Framework Filter, and Compliance Control Filter. In terms of audits relating to security updates and patches, we can search for several related controls.

Related Controls: 800-53r5 SI-2*, 800-171 3.14.1, CIS CSC v7 3.4, 3.5/ CIS CSC v8 7.3, 7.4, CSF ID.RA-1/PR.IP-12, ISO-27001 A.12.6.1

Tenable Vulnerability Management

With the related controls in mind, the next step is to navigate to Tenable Vulnerability Management's Findings page. In the Host Audits section of the Findings the user can use the Audit Check Name filter to find relevant audit results. When searching for patch-related controls, the Audit Check Name may contain keywords like patches or updates.



To further enhance the query, the Audit Check Name filter can be used in combination with the Compliance Framework Filter and the Compliance Control Filter. This combination ensures a more targeted search is performed.

Findings

Vulnerabilities | Cloud Misconfigurations | **Host Audits** | Web Application Findings

Advanced | Saved Filters | Search by Asset Name, IP, IP Range, or a CIDR, * for wildcard

Audit Check Name: is equal to *updates* × | Compliance Control: is equal to 7.3 × | Compliance Framework: is equal to CSCv

Filters

Apply

Select Filters | Reset

Audit Check Name

is equal to

updates

Compliance Control

is equal to

7.3

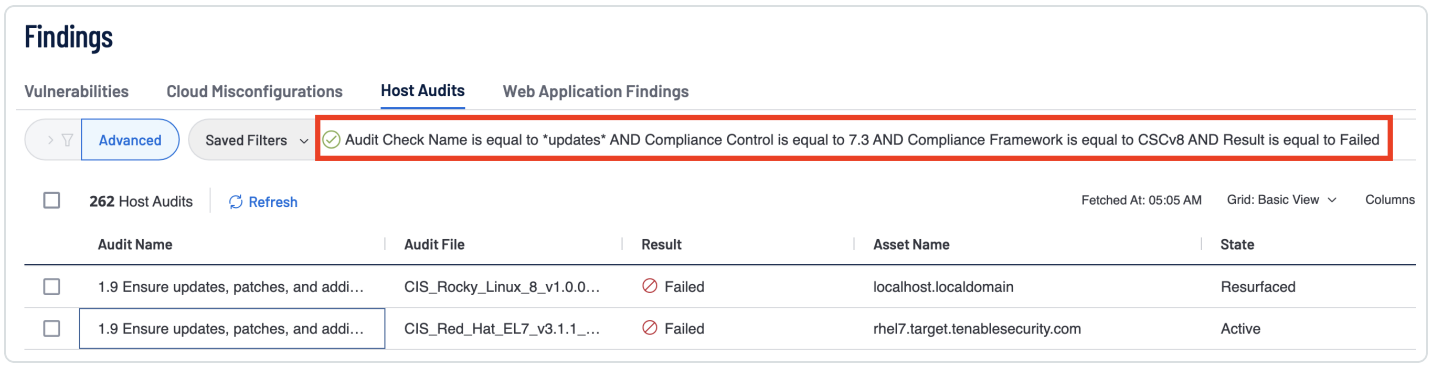
Compliance Framework

is equal to

CSCv8

340 Host Audits | Refresh

Audit Check Name
1.9 Ensure updates, patches, an…
1.9 Ensure updates, patches, an…
1.9 Ensure updates, patches, an…
18.9.108.4.3 Ensure 'Select whe…
1.5 Ensure System Data Files an…
18.9.108.2.2 Ensure 'Configure A…
18.9.108.1.1 Ensure 'No auto-res…
1.9 Ensure updates, patches, an…
18.10.93.2.1 Ensure 'Configure A…
18.10.93.2.2 Ensure 'Configure A…
18.9.108.1.2 Ensure 'Do not disp…
1.9 Ensure updates, patches, an…
18.10.93.4.3 Ensure 'Select whe…
18.10.93.4.3 Ensure 'Select whe…

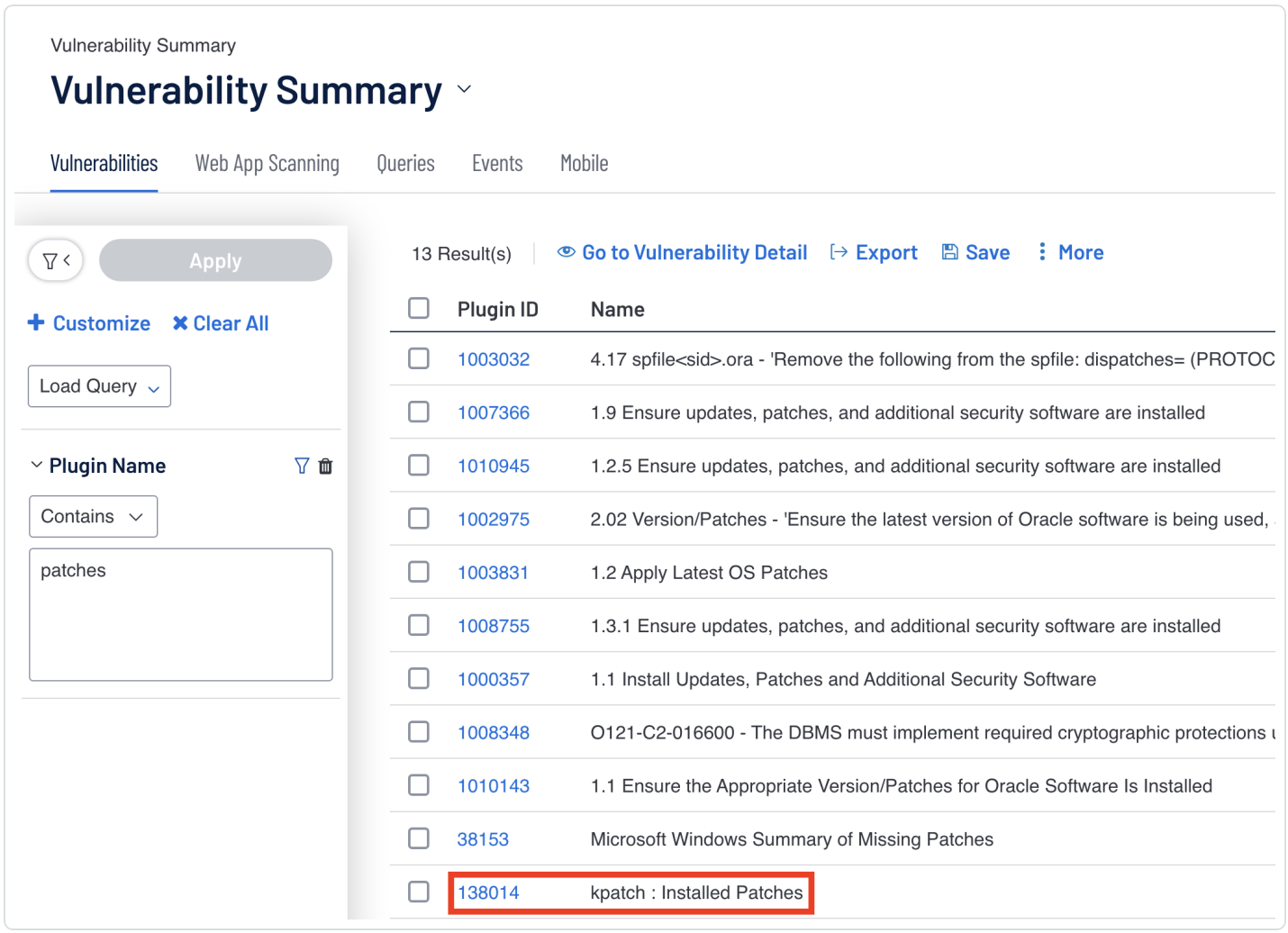


The previous query can be replicated by selecting the “Advanced button” within the Host Audits section of the findings page and inputting the following queries:

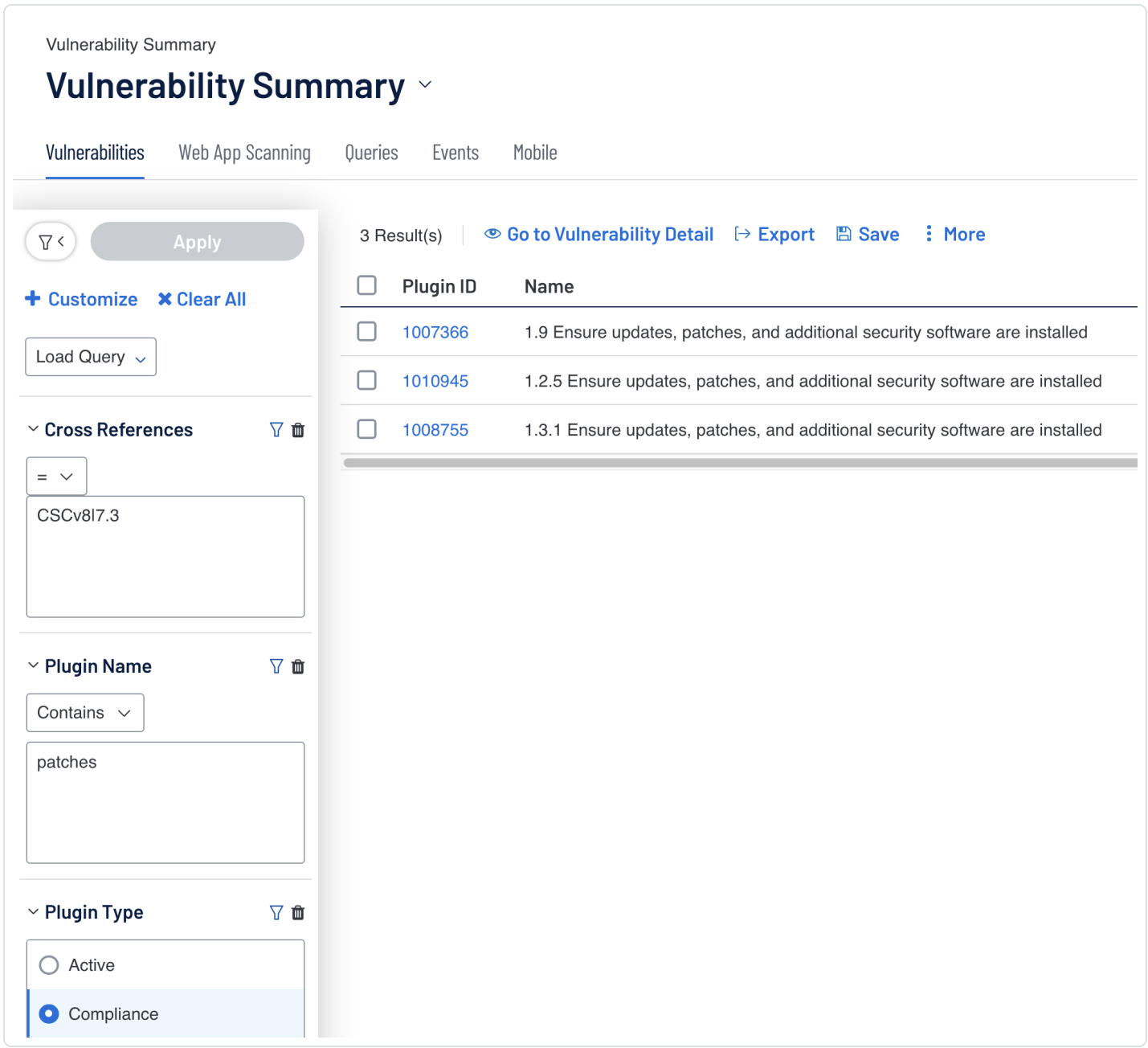
- Audit Check Name is equal to *updates* AND Compliance Control is equal to 7.3 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *patches* AND Compliance Control is equal to 7 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *Automatic Updates* AND Compliance Control is equal to 7 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed

Tenable Security Center

In Tenable Security Center a user will want to navigate to the Analysis page for their queries. When querying in Tenable Security Center, the audit check name becomes the plugin name. This means that just searching for keywords in a plugin name alone would result in possibly many **false positives** being returned.



In the previous example, searching for Plugin Name contains “patches” results in a false positive which can adversely affect compliance tracking. To reduce the number of possible false positives, the user will want to use other filters like the Plugin Type filter set to compliance, and the Cross Reference filter to grab only results related to the relevant framework and control. These filters enhance the query to enable the user to establish a focused and precise search.



Account Management

Account Management is also imperative, as enterprise assets and software are just as secure as the users that use them. The most common methods of attack tend to be targeting the users of the systems themselves, as the user's access may lead the attacker to other assets and systems. Ensuring that users only have the appropriate level of permissions and access to certain file directories can help secure the accounts themselves. An administrator user should also have an account with appropriate and non-admin level privileges if they also use the system outside of admin duties. The presence of default accounts and passwords may be targets for attackers. This

should be prevented by removing them entirely. Another configuration settings that can be set are screen lock and logout settings, as these can greatly increase the security of workstations.

Dealing with user passwords is also an important aspect in account management that will help set up a secure configuration. Password length and complexity requirements should help eliminate default passwords and ensure that user passwords are not as easily identified. Interactive logon is a necessity in many security guidelines including CIS benchmarks, as well as the implementation of time between login attempts or a set number of consecutive failed attempts before an account is locked. These password requirements make it tougher for threat actors to utilize password guessing tools which try many different combinations and/or dictionaries of passwords to gain access to the user account.

Questions that this section may help solve:

1. **A screen lock or a logout should be implemented to the workstations when leaving the work area. Which audits will help identify this?**
2. **Screensaver should be protected by a password with a timeout period. Can tenable assist in verifying this?**
3. **Only authorized persons should access the systems. How can I verify this? (permissions/access level)**
4. **Administrator group should be verified and maintained. How can I verify this?**

Search Examples

The Audit Check Name filter in Tenable Vulnerability Management and the Plugin Name filter in Tenable Security Center are useful filters that allow a user to be specific with which checks they want to look at. For example, Control 4.3 is “Configure Automatic Session Locking on Enterprise Assets.” Some example audit checks are; "5.5.5 Ensure default user shell timeout is 900 seconds or less", "1.4.1 Ensure 'Idle timeout' is less than or equal to 10 minutes for device management", and "5.4.5 Ensure default user shell timeout is 900 seconds or less - /etc/profile". These audit checks show us a common word that is used often when testing for CSCv8 4.3 compliance… “timeout”.

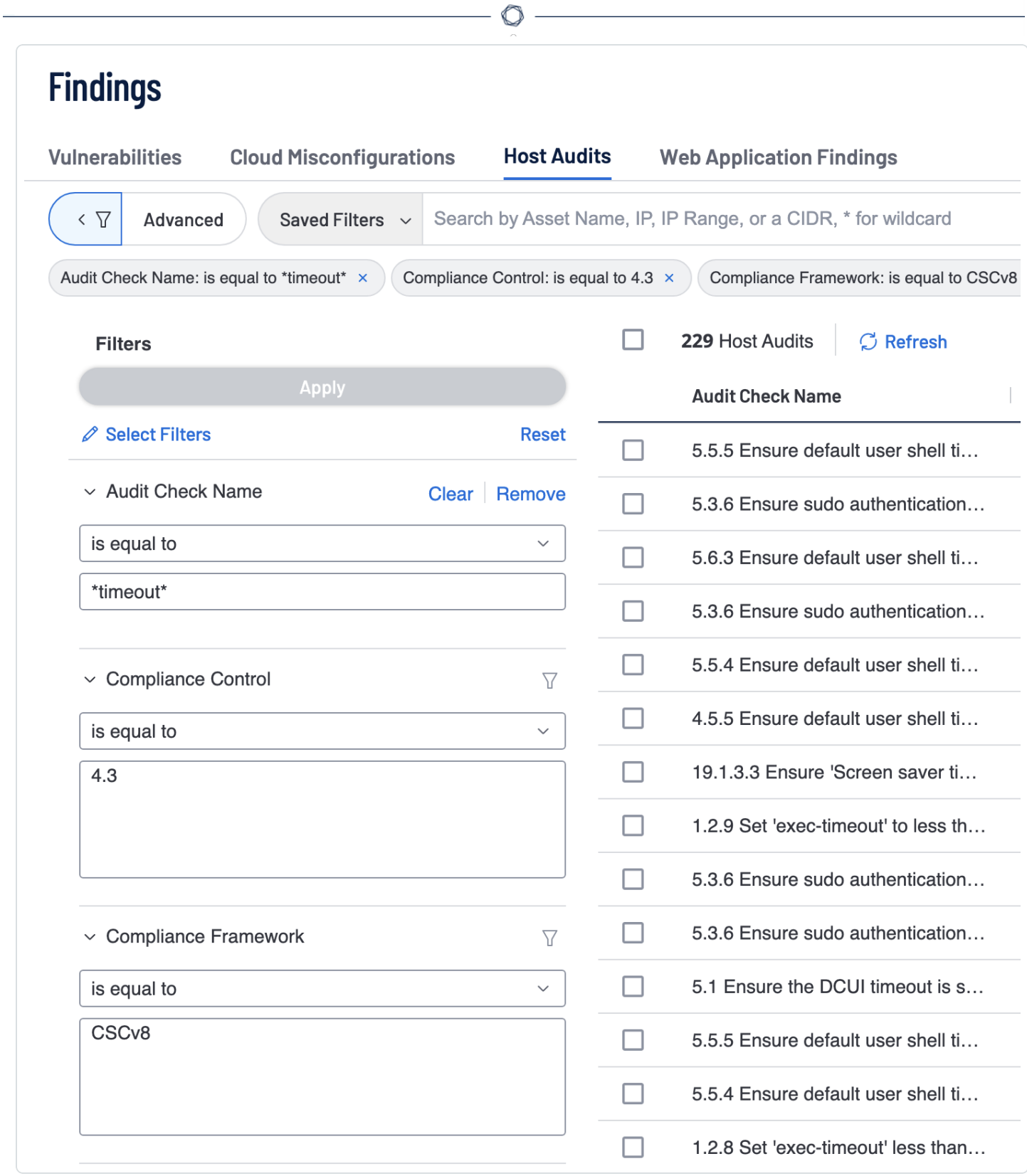
Keyword	Common Windows Audit Name	Common Unix Audit Name
Rename	"2.3.1.4 Configure 'Accounts: Rename administrator account'"	"10.5 Rename the manager application - host-manager/manager.xml"

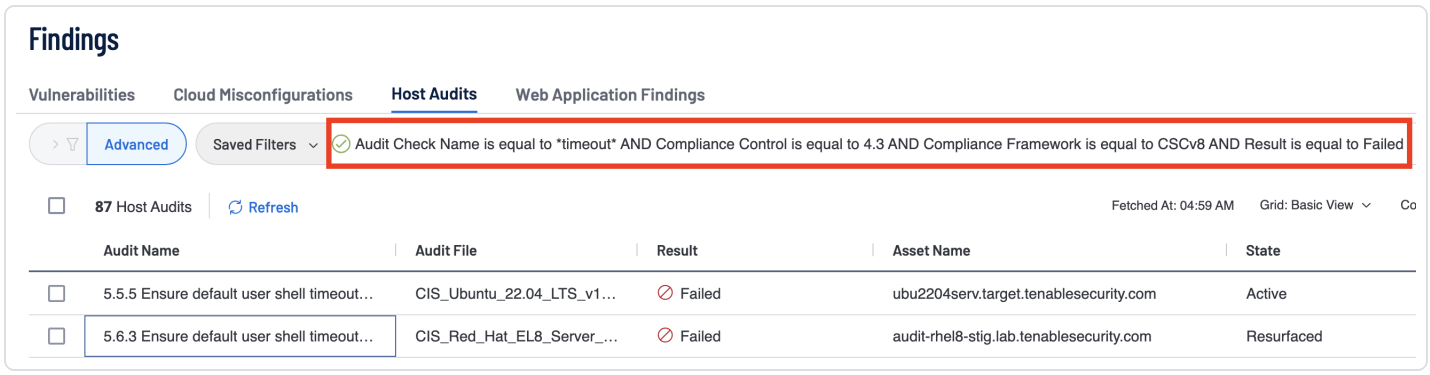
Guest Account	"2.3.1.2 Ensure 'Accounts: Guest account status' is set to 'Disabled'"	"2.3.1.5 Configure 'Accounts: Rename guest account' - Accounts: Rename guest account"
timeout	"Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'"	"5.5.5 Ensure default user shell timeout is 900 seconds or less"
timeout	"Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'"	"5.5.5 Ensure default user shell timeout is 900 seconds or less"
Interactive Log	"2.3.7.4 Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0'"	N/A
Lockout	N/A	"4.4 Ensure account lockout is set to 15 minutes"
Lock	"18.9.87.1 Ensure 'Sign-in and lock last interactive user automatically after a restart' is set to 'Disabled'"	"1.8.4 Ensure GDM screen locks when the user is idle"
Screen saver	"19.1.3.2 Ensure 'Password protect the screen saver' is set to 'Enabled'"	N/A

Note: When searching a keyword in Tenable Security Center (Plugin Name filter), the plugin type compliance filter should be used along with a cross reference filter to eliminate any false positives in the query.

Tenable Vulnerability Management

With the keywords in mind, the user can head over to the Findings -> Host Audit page in Tenable Vulnerability Management and utilize the Audit Check Name Filter in combination with the Compliance Control Filter and Compliance Framework filters to find similar audit checks. The Query could be like: “Audit Check Name eq *timeout*Compliance Control is equal to 4.3, and Compliance Framework equals CSCv8.”


Findings
Vulnerabilities
Cloud Misconfigurations
Host Audits
Web Application Findings
Advanced
Saved Filters
Search by Asset Name, IP, IP Range, or a CIDR, * for wildcard
Audit Check Name: is equal to *timeout*
Compliance Control: is equal to 4.3
Compliance Framework: is equal to CSCv8
Filters
Apply
Select Filters
Reset
Audit Check Name
Clear
Remove
is equal to
timeout
Compliance Control
is equal to
4.3
Compliance Framework
is equal to
CSCv8
229 Host Audits
Refresh
Audit Check Name
5.5.5 Ensure default user shell ti…
5.3.6 Ensure sudo authentication…
5.6.3 Ensure default user shell ti…
5.3.6 Ensure sudo authentication…
5.5.4 Ensure default user shell ti…
4.5.5 Ensure default user shell ti…
19.1.3.3 Ensure 'Screen saver ti…
1.2.9 Set 'exec-timeout' to less th…
5.3.6 Ensure sudo authentication…
5.3.6 Ensure sudo authentication…
5.1 Ensure the DCUI timeout is s…
5.5.5 Ensure default user shell ti…
5.5.4 Ensure default user shell ti…
1.2.8 Set 'exec-timeout' less than…

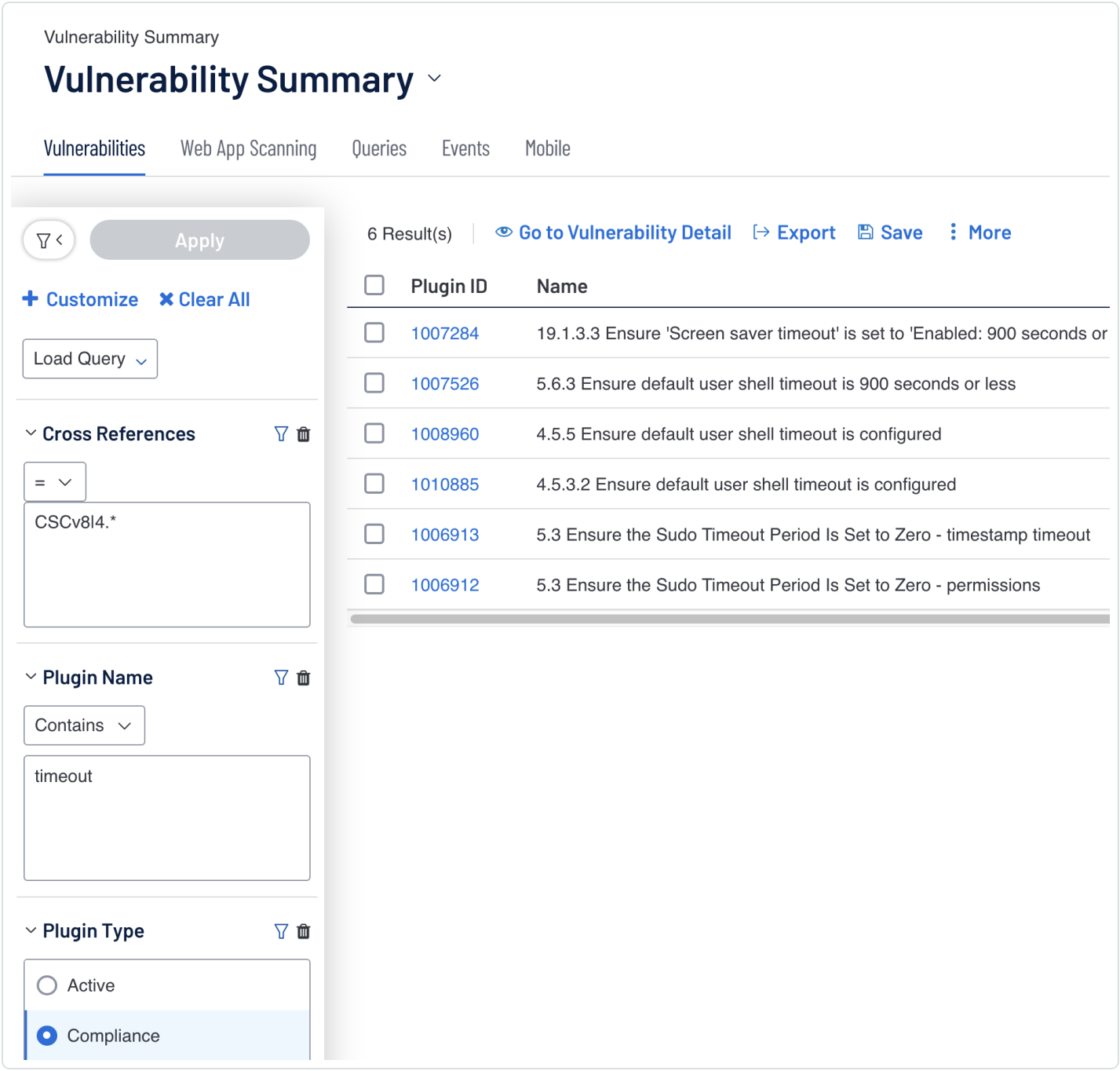


The previous query can be replicated by selecting the “Advanced button” within the Host Audits section of the findings page and inputting the following queries: “Audit Check Name is equal to *audit log* AND Compliance Control is equal to 8.3 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed.”

- Audit Check Name is equal to *audit log* AND Compliance Control is equal to 8.3 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *Interactive Log* AND Compliance Control is equal to 8 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *Lockout* AND Compliance Control is equal to 8 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed

Tenable Security Center

When targeting audit checks that will include checks run related to account management, we can use the Cross Reference filter in Tenable Security Center to target specific controls within a framework. In this case the focus would be Critical Security Controls v8 (CSCv8) Control 4. In Tenable Security Center the query could be “CSCv8|4.*” This would cover all the audit checks related to control 4. The query can be even more targeted by specifying the control further: for example, “CSCv8|4.7” would result in checks dealing with the management of default account on enterprise assets.



Resource Control

Having secure configuration can also include setting file permissions to their appropriate values based on the user. File permissions that are incorrectly setup can lead to directories being exposed to modification from certain users that shouldn't have access. These exposed directories can lead to unintentional or intentional breaches. To remedy this issue, the security team can ensure denying read access to certain files or entire directory trees; this will ensure the confidentiality of the files. To protect the integrity of the file system, write access can also be removed for users not

needing it. Lastly, removing the execution privilege or limiting privilege to administrative users can assist in preventing a possibly compromised user from taking advantage.

It is also possible to create virtual environments that will contain server processes or user actions within them, so the overall integrity of the system can be more easily maintained. One example of this in Unix is utilizing the "chroot" command which will move the current running process from the apparent root directory. With the command the process is unable to access any files outside of the environment.

Search Examples

Questions that this section may help solve:

1. **Principle of least privilege... How can tenable help verify this?**

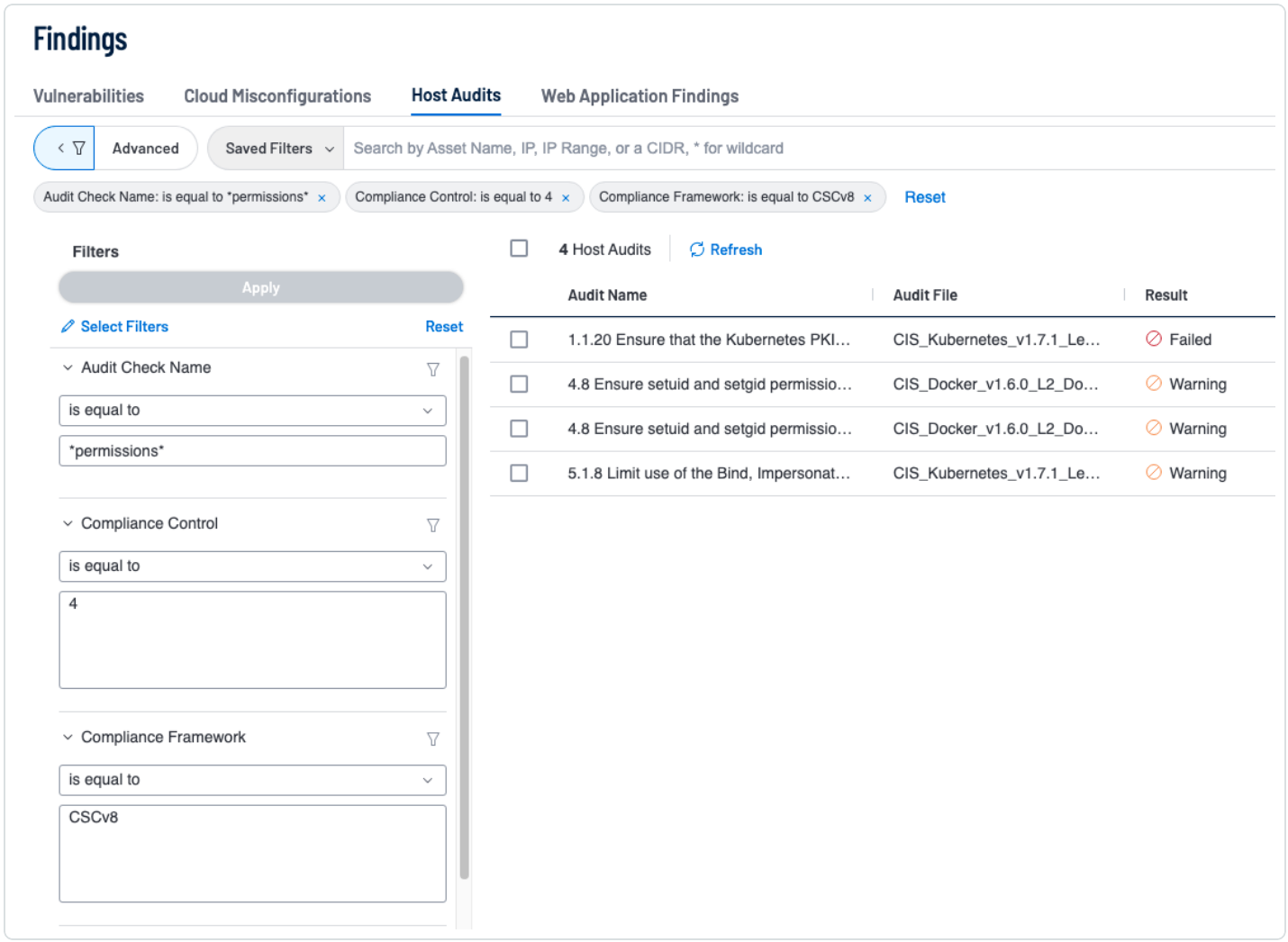
Keyword	Common Windows Audit Name	Common Unix Audit Name
permissions	"1.4.2 Ensure permissions on bootloader config are configured - grub.cfg"	"2.3.10.7 Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'"
files	"20.61 Ensure 'Software certificate installation files must be removed'"	"1.1.1.1 Ensure mounting of cramfs filesystems is disabled - modprobe"
Environment	"2.2.32 Ensure 'Modify firmware environment values' is set to 'Administrators'"	"5.2.10 Ensure SSH PermitUserEnvironment is disabled - sshd output"

Note: When searching a keyword in Tenable Security Center (Plugin Name filter), the plugin type compliance filter should be used along with a cross reference filter to eliminate any false positives in the query.

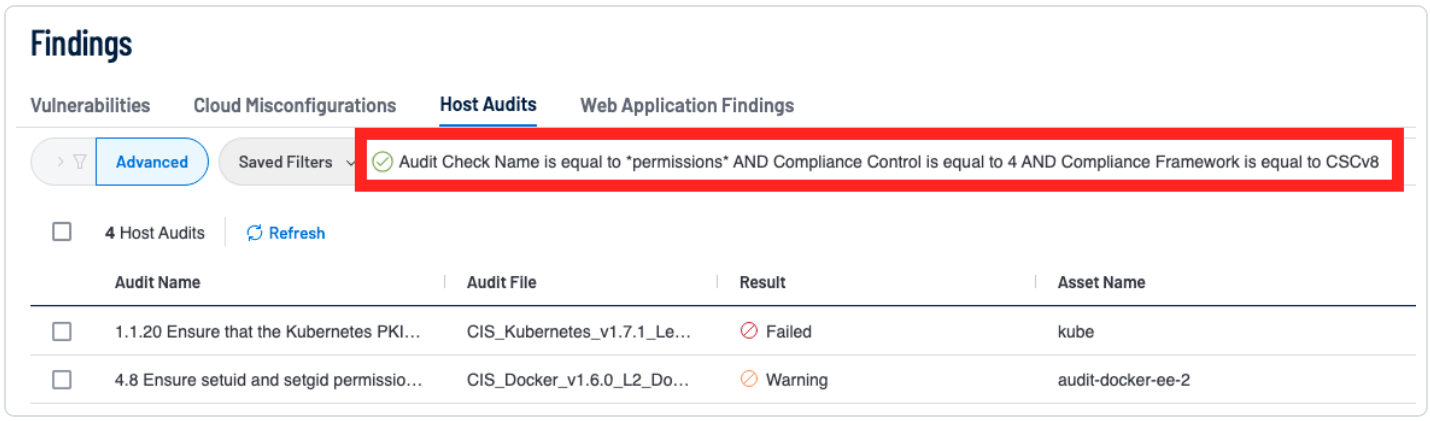
Tenable Vulnerability Management

Taking into account the need for permissions to be correctly set within accounts, the user can use the keyword "permissions" to focus on permissions related audit checks. With the keyword in mind, the user can input the keyword in Tenable Vulnerability Management using the Audit Check Name filter. After using the Audit Check Name filter the user can benefit from using the Compliance

Framework filter and/or the Compliance Control; both of these filters can specify which audit checks the query filters by only including the desired framework and/or control. In this case, the user sets the Compliance Framework filter equal to “CSCv8” and the Compliance Control filter equal to 4. This query ensures all Audit Checks that include the word “permissions” in the name and are part of the CIS CSCv8 Control 4 are shown.



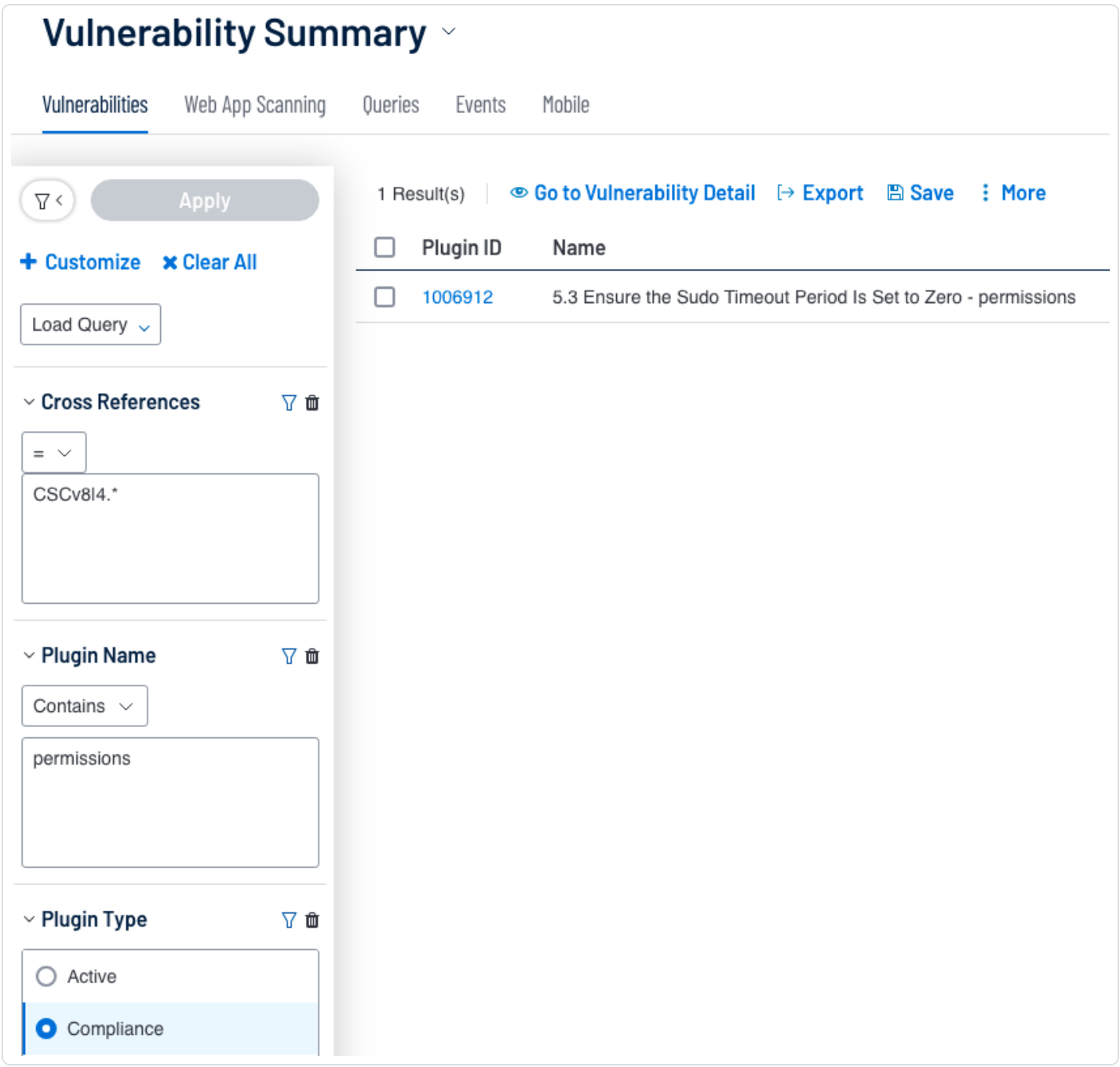
The following Advanced Query can be replicated by selecting the “Advanced button” within the Host Audits section of the findings page and inputting the following queries: “Audit Check Name is equal to *permissions* AND Compliance Control is equal to 4 AND Compliance Framework is equal to CSCv8”.



- Audit Check Name is equal to *permissions* AND Compliance Control is equal to 4 AND Compliance Framework is equal to CSCv8
- Audit Check Name is equal to *files* AND Compliance Control is equal to 4 AND Compliance Framework is equal to CSCv8

Tenable Security Center

Following the previous example, the user can query the same results in Tenable Security Center. Instead of the Audit Check Name filter, Tenable Security Center has the Plugin Name filter, and for the compliance-related filters the user can use the Cross Reference Filter. In this case the user sets the Plugin Name Filter to contain “permissions." Much like in Tenable Vulnerability Management, just using the keyword to filter out the results may lead to false positives. So, to combat the false positives with searching by plugin name, the user can use the Plugin Type filter set to Compliance, and the Cross Reference Filter set to equals “CSCv8|8.*”. This query also ensures that all Audit Checks that include the word “permissions” in the name and are part of the CIS CSCv8 Control 4 are shown.


Vulnerability Summary
Vulnerabilities
Web App Scanning
Queries
Events
Mobile
Apply
Customize
Clear All
Load Query
Cross References
=
CSCv8l4.*
Plugin Name
Contains
permissions
Plugin Type
Active
Compliance
1 Result(s)
Go to Vulnerability Detail
Export
Save
More
Plugin ID
Name
1006912
5.3 Ensure the Sudo Timeout Period Is Set to Zero - permissions

Log Collection and Management

Questions that this section may help solve:

1. **How do I ensure Logs are capturing when confidential information is being read/updated (ex. Passwords)?**
2. **Do my logs show who or what performed the action on my system?**
3. **The changing of access rights (revocation/Grants/modifying) should be logged. Which audits will help me identify this compliance?**
4. **Apps startup/shutdown/restart/abort/failure/or abnormal end should also be logged. How can this be verified with compliance scanning?**
5. **Logs should be sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system. Which audits will verify the presence of these protocols?**

Ensuring logging is appropriately set up and operating correctly is important when securing enterprise assets, as this helps identify potential attacks. In some instances, analyzing the logs may be the only way to prove an attack was carried out successfully. In many cases an attacker is aware that most enterprises may be logging activities, though most do not analyze the logs in a regular enough frequency. This irregular log analysis can allow an attacker to be exploiting the system for weeks, months, or more without detection.

There are two common types of logs; Audit Logs and system logs. Audit logs usually include user-level events, while system logs have system-level events. System logs are usually easier to enable as they may require less configuration, while audit logs take more configuration, as they involve collecting information on when users access certain files, logged in, etc.

Search Examples

When attempting to focus on Audit log compliance results one thing that can be helpful is to have specific controls or audit checks in mind to query within Tenable Vulnerability Management or Tenable Security Center. Refer to the Search Overview Section for a refresher on audit file format and structure. Focusing on Audit Log management and confirming the enterprise's compliance can be done more efficiently if common keywords for audit checks are used to query through the compliance scan results. In the Keyword table are some common keywords that can be found as audit checks related to audit log management.

Keyword	Common Windows Audit Name	Common Unix Audit Name
Audit Log	"17.5.3 Ensure 'Audit Logoff' is set to include 'Success'"	"4.1.1.1 Ensure audit log storage size is configured"
System Logs	N/A	"4.1 (L1) Host must configure a persistent log location for all locally stored system logs"
Logging	"Turn on PowerShell Script Block Logging - EnableScriptBlockInvocationLogging"	"5.3 Ensure that logging captures as much information as possible"
Logs	"Windows Defender Firewall: Allow logging - LogSuccessfulConnections"	"3.1.7 Secure permissions for all diagnostic logs"

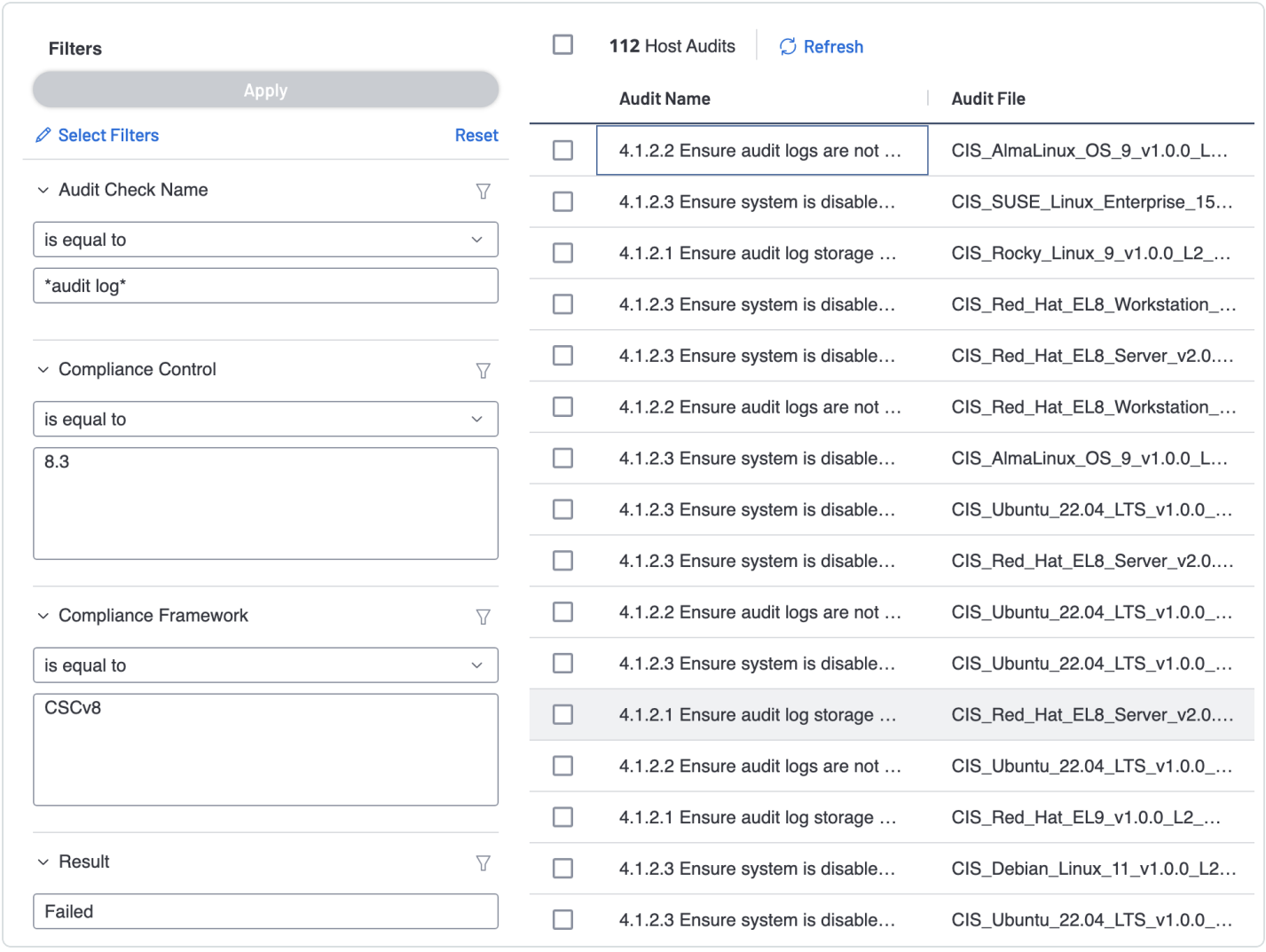
Note: When searching a keyword in Tenable Security Center (Plugin Name filter), the plugin type compliance filter should be used along with a cross reference filter to eliminate any false positives in the query.

Related Controls: 800-53r5 AU-9*, 800-171 3.3.*, CIS CSC v7 6.4, 6.5/ CIS CSC v8 8.3, 8.9, CSF PR.DS-4, PR.PT-1, ISO-27001 A.6.1.2,A.9.4.1,A.9.4.5

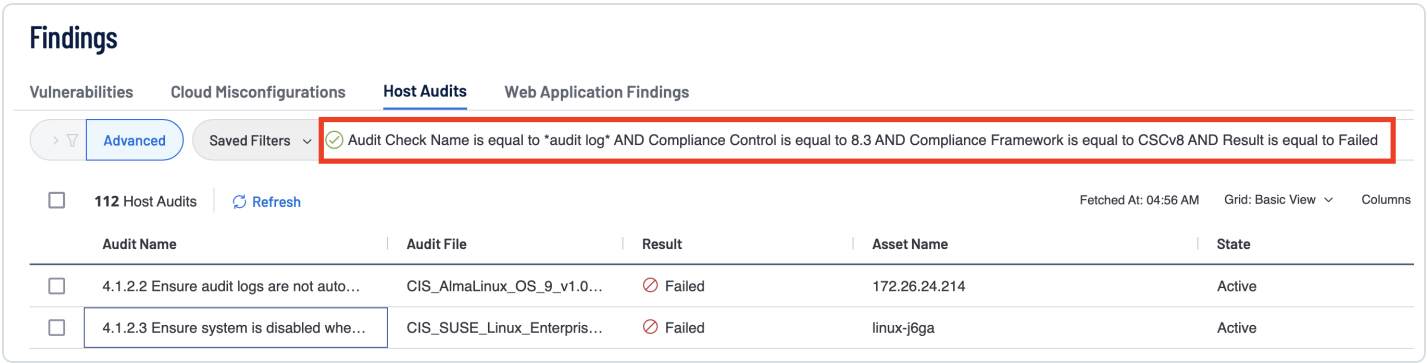
Tenable Vulnerability Management

In Tenable Vulnerability Management the user can navigate to the Findings page and Host Audits section to query results from the Policy Compliance scan that was run. Once there, the filters that are most useful to use are the Compliance Framework, Compliance Control, and Audit Check Name filters. An additional filter that can be useful in conjunction with the others is the Results filter, as the filter allows the user to focus on different states of compliance for the assets.

For example, the focus may be tracking the state of compliance and more specifically grabbing a list of failed checks involving audit logs in Windows and Unix assets. For this scenario the user will want to focus on Failed Result types using the Result Filter. In Tenable Vulnerability Management the user could use the Compliance Control filter equal to 8.3, Compliance Framework filter equal to “CSCv8”, Result set to Failed, and Audit Check Name filter equal to *audit log*. One important note is that the asterisks need to be in the Audit Check Name filter value so the filter acts as a contains rather than a straight match.



This query can be replicated by selecting the “Advanced” button within the Host Audits section of the findings page and inputting the following queries:

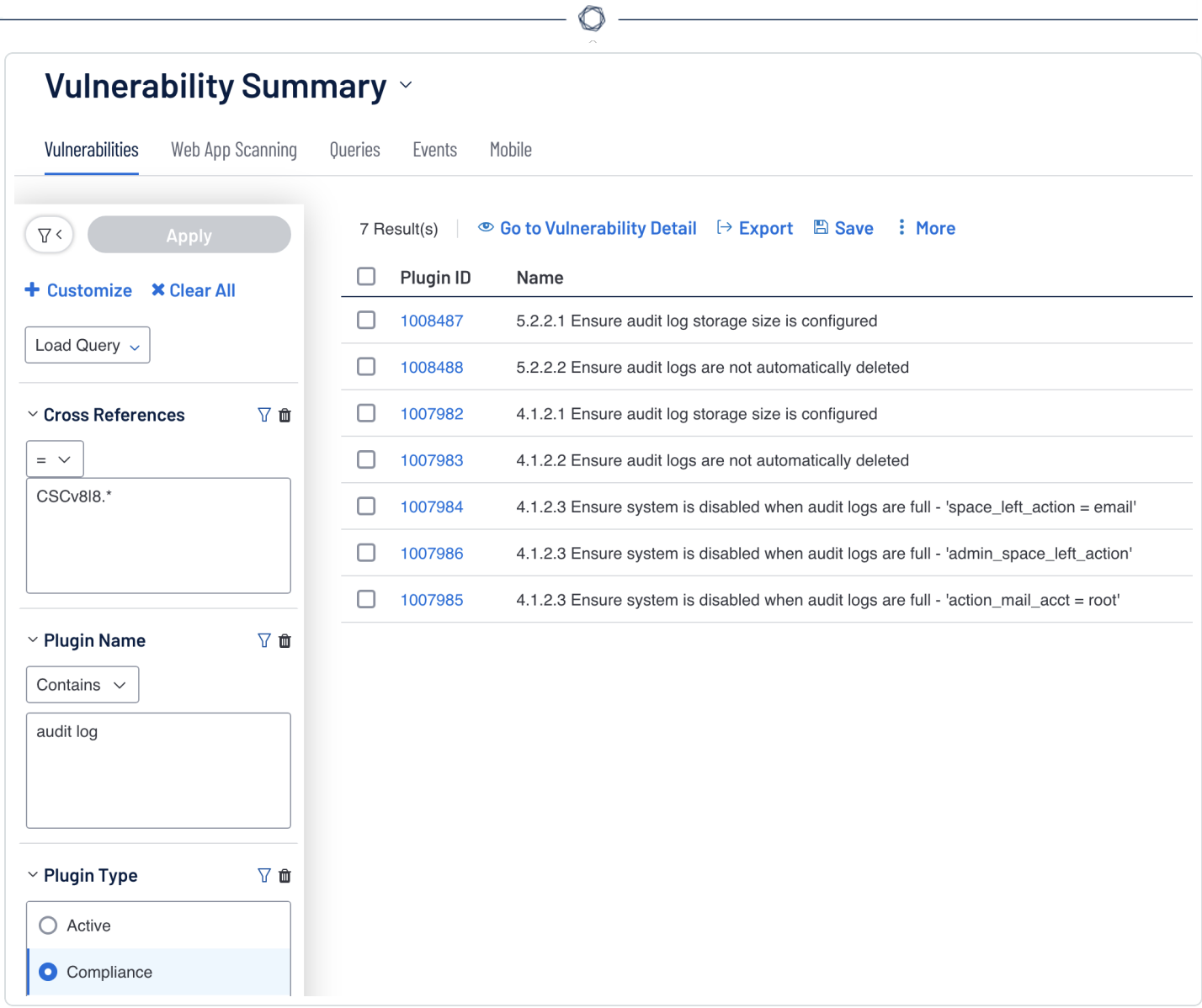


- Audit Check Name is equal to *audit log* AND Compliance Control is equal to 8.3 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *System Logs* AND Compliance Control is equal to 8 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *Logging* AND Compliance Control is equal to 8 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed

Tenable Security Center

In Tenable Security Center the user needs to navigate to the Analysis page and use the Plugin Type filter, Plugin Name Filter, and Cross Reference Filter. The Plugin Type filter needs to be set to 'Compliance' to focus only on compliance plugins and results. The Plugin Name filter can be set to contains and whatever keyword the user may need; like in the previous example the keywords can be "Audit log" so the query looks at audit checks that have "audit log" in the name. Lastly, the Cross Reference filter allows the user to further filter the results by Compliance Framework and Compliance Control.

Following the previous scenario covered in the Tenable Vulnerability Management section, the user will want to focus on Failed Result types which can be achieved by using the Severity filter set to High. The next filters the user will use are Plugin type set to compliance, cross reference equal to "CSCv8|8.*", and Plugin Name contains "audit log". Be aware that the asterisk in the Cross Reference filter is used to cover any check that is related to control 8.


Vulnerability Summary
Vulnerabilities
Web App Scanning
Queries
Events
Mobile
Apply
Customize
Clear All
Load Query
Cross References
=
CSCv8l8.*
Plugin Name
Contains
audit log
Plugin Type
Active
Compliance
7 Result(s)
Go to Vulnerability Detail
Export
Save
More
Plugin ID
Name
1008487
5.2.2.1 Ensure audit log storage size is configured
1008488
5.2.2.2 Ensure audit logs are not automatically deleted
1007982
4.1.2.1 Ensure audit log storage size is configured
1007983
4.1.2.2 Ensure audit logs are not automatically deleted
1007984
4.1.2.3 Ensure system is disabled when audit logs are full - 'space_left_action = email'
1007986
4.1.2.3 Ensure system is disabled when audit logs are full - 'admin_space_left_action'
1007985
4.1.2.3 Ensure system is disabled when audit logs are full - 'action_mail_acct = root'

Network Hardening and Monitoring

Questions that this section may help solve:

1. **A firewall must be present between DMZ lab and internet. How can I verify this?**
2. **Disable unencrypted remote admin protocols used to manage network infrastructure (for example, Telnet, File Transfer Protocol [FTP]). What will I do to verify compliance?**
    a. **Disable unnecessary services (for example, discovery protocols, source routing, Hypertext Transfer Protocol [HTTP], Simple Network Management Protocol [SNMP], Bootstrap Protocol).**
3. **I should protect routers and switches by controlling access lists for remote administration, how can I verify compliance.**

Quick Overview: Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Much like enterprise assets and software, secure network infrastructure is not secure by default. The out-of-the-box configuration is tailored for ease-of-use and/or ease-of-deployment. This lack of a secure configuration can lead to a network at risk of being breached and exploited. Network infrastructure includes physical and virtualized devices like firewalls, routers, switches, and access points. Open services or older and vulnerable protocols should be vetted and determined whether they should be disabled. Much like in desktop workstations, default accounts and passwords need to also be maintained as they may usually be the first avenue of attack.

Assessing network security is an always changing environment which necessitates regular re-assessment. The regular re-assessment is important because a would-be attacker is constantly looking for gaps or inconsistencies in firewall rule sets, default configurations, routers, and switches that the attacker then uses to nullify the defenses.

Secure network infrastructure is an essential defense against attacks. This includes an appropriate security architecture, addressing vulnerabilities that are oftentimes introduced with default settings, monitoring for changes, and reassessment of current configurations. Network infrastructure includes devices such as physical and virtualized gateways, firewalls, wireless access points, routers, and switches. The attackers hope and take advantage of the fact that network device configurations weaken over time and, therefore, become exploitable. This expectation of a

weakening configuration overtime makes regular auditing crucial to stay ahead of the curve and protect enterprise assets and software.

Search Examples

Attempting to confirm compliance with network hardening and monitoring can be done by searching through the audit file for certain related keywords. For example, words like “Access-list”, “packet”, or “Network” can result in audit checks that may be useful to the user. Once again, do not just use the keyword or phrase as the sole filter when querying through the data. Using just the keyword may result in false positives and unrelated results or plugins to come up. The following Keyword table shows just a few common keywords that can be used when trying to focus on Network hardening-related audit checks.

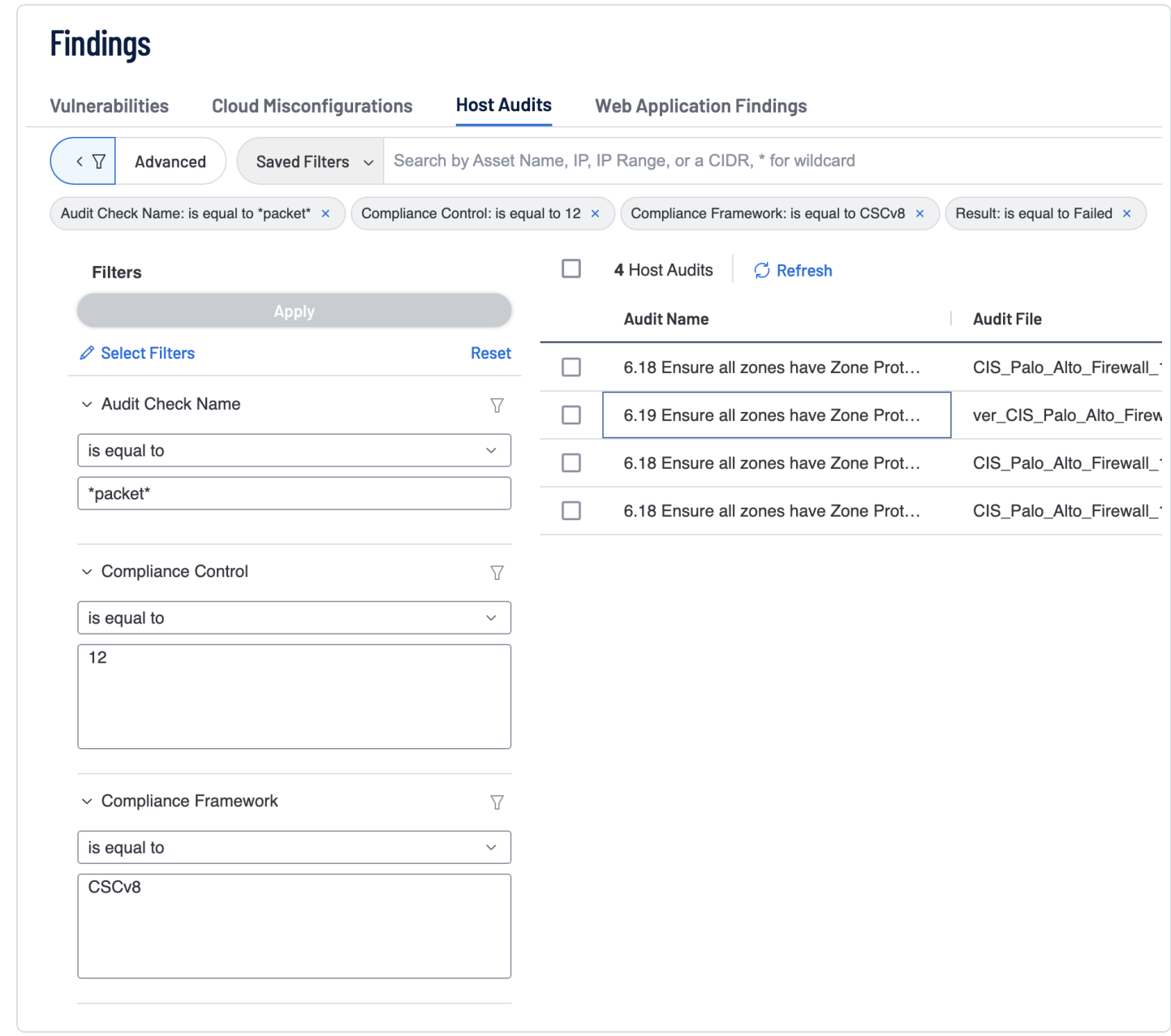
Keyword	Common Windows Audit Name	Common Unix Audit Name	Common Networking Audit Name
Access-list	N/A	N/A	"3.2.1 Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks - 'Deny internal networks'"
Packet	"3.1.2 Ensure packet redirect sending is disabled - sysctl ipv4 all send"	"9.3.8 (L1) Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'"	"Ensure source routed packets are not accepted - /etc/sysctl ipv4 default accept"
Network	"2.3.11.2 Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'"	"3.2.1 Set 'ip access-list extended' to Forbid Private Source Addresses from External Networks - 'Deny internal networks'"	"Ensure events that modify the system's network environment are collected - auditctl /etc/sysconfig/network"
firewall	"Windows Defender Firewall: Protect all network connections"	"3.5.1.4 Ensure firewall rules exist for all open ports"	"Ensure default deny firewall policy - Chain OUTPUT"

> **Note:** When searching a keyword in Tenable Security Center (Plugin Name filter), the plugin type compliance filter should be used along with a cross reference filter to eliminate any false positives in the query.

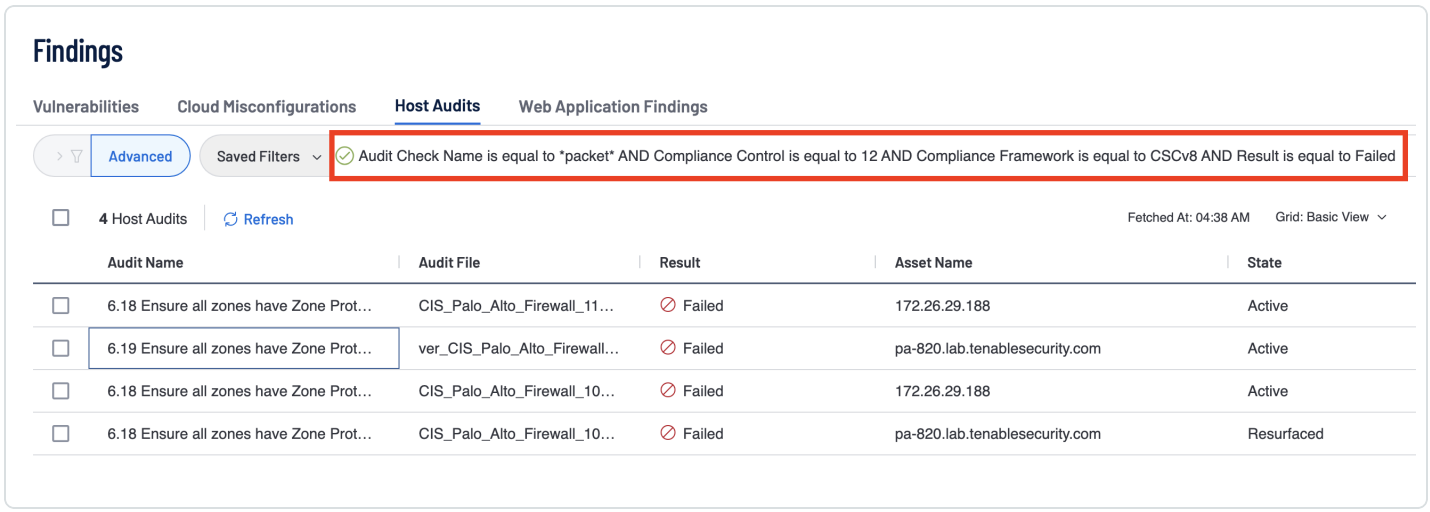
Related Controls: 800-53r5 AU-9*, 800-171 3.3.*, CIS CSC v7 6.4, 6.5/ CIS CSC v8 8.3, 8.9, CSF PR.DS-4,PR.PT-1, ISO-27001 A.6.1.2,A.9.4.1,A.9.4.5

Tenable Vulnerability Management

As an example, we can focus on trying to confirm compliance with firewall rules setup. In this example we'll focus on failed audit checks so we can track what needs to be fixed. In Tenable Vulnerability Management the first filter that we'll use is the Audit Check Name filter equal to "*packet*". This filter returns all audit checks that include the word packet. To eliminate any false positives, we can add the two filters: the Compliance Framework filter equal to CSCv8 and the Compliance Control filter equal to "12". Lastly, to eliminate passed checks the user can use the Result filter equal to Failed.



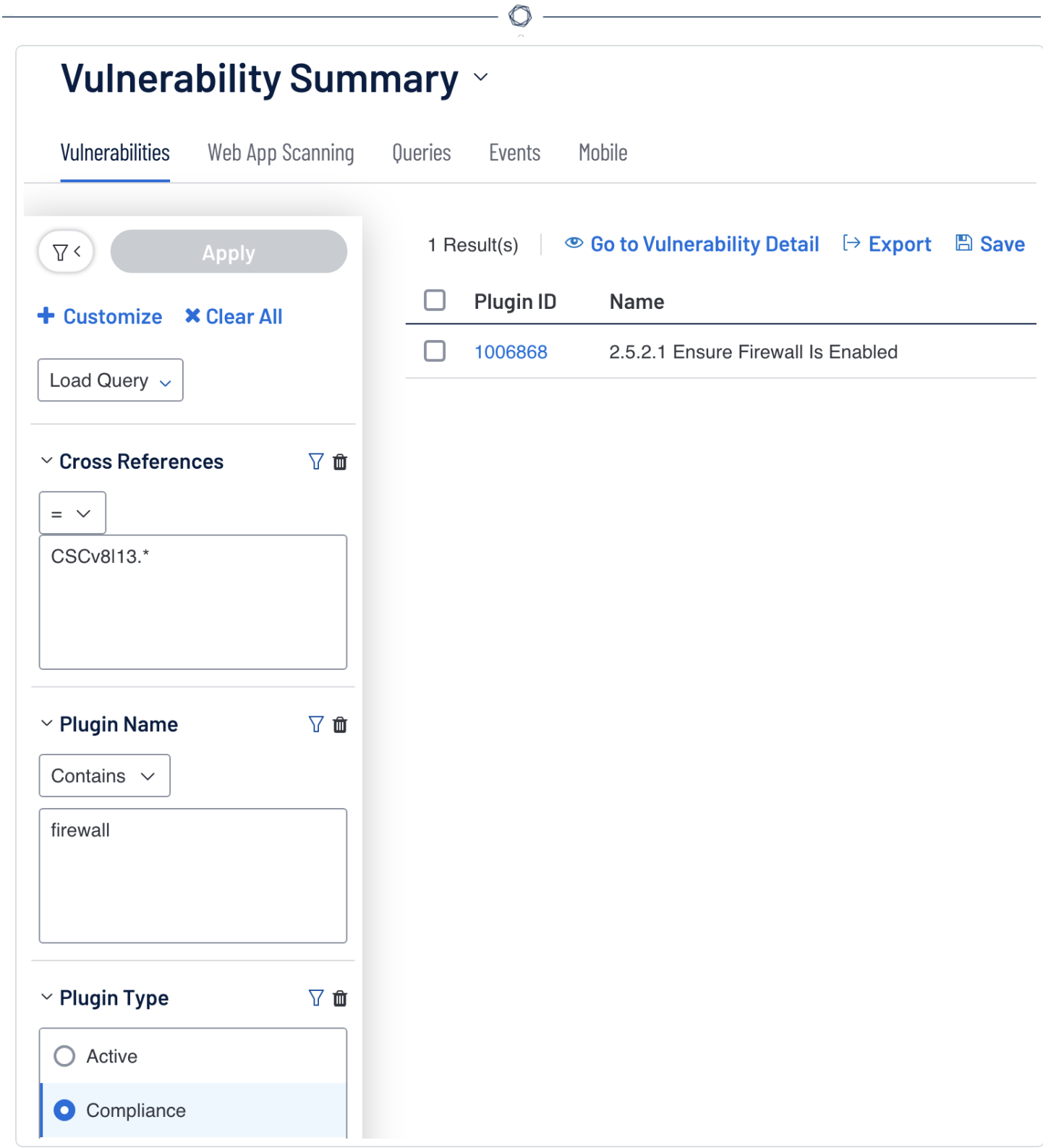
This query can be replicated by selecting the “Advanced” button within the Host Audits section of the findings page and inputting the following queries:



- Audit Check Name is equal to *packet* AND Compliance Control is equal to 12 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *Network* AND Compliance Control is equal to 12 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed
- Audit Check Name is equal to *Access-list* AND Compliance Control is equal to 12 AND Compliance Framework is equal to CSCv8 AND Result is equal to Failed

Tenable Security Center

In Tenable Security Center, following a similar example as in the previous section, the user uses the Plugin Name filter contains firewall, along with Plugin Type set to compliance. While the plugin type filter eliminates some false positives, in Tenable Security Center the user can utilize the Cross Reference filter to enhance the query to include only the target compliance framework and control. In this example the Cross Reference filter can be set to equals “CSCv8|13.*”.


Vulnerability Summary
Vulnerabilities
Web App Scanning
Queries
Events
Mobile
Apply
Customize
Clear All
Load Query
Cross References
=
CSCv8I13.*
Plugin Name
Contains
firewall
Plugin Type
Active
Compliance
1 Result(s)
Go to Vulnerability Detail
Export
Save
Plugin ID
Name
1006868
2.5.2.1 Ensure Firewall Is Enabled

Widget/Component Creation

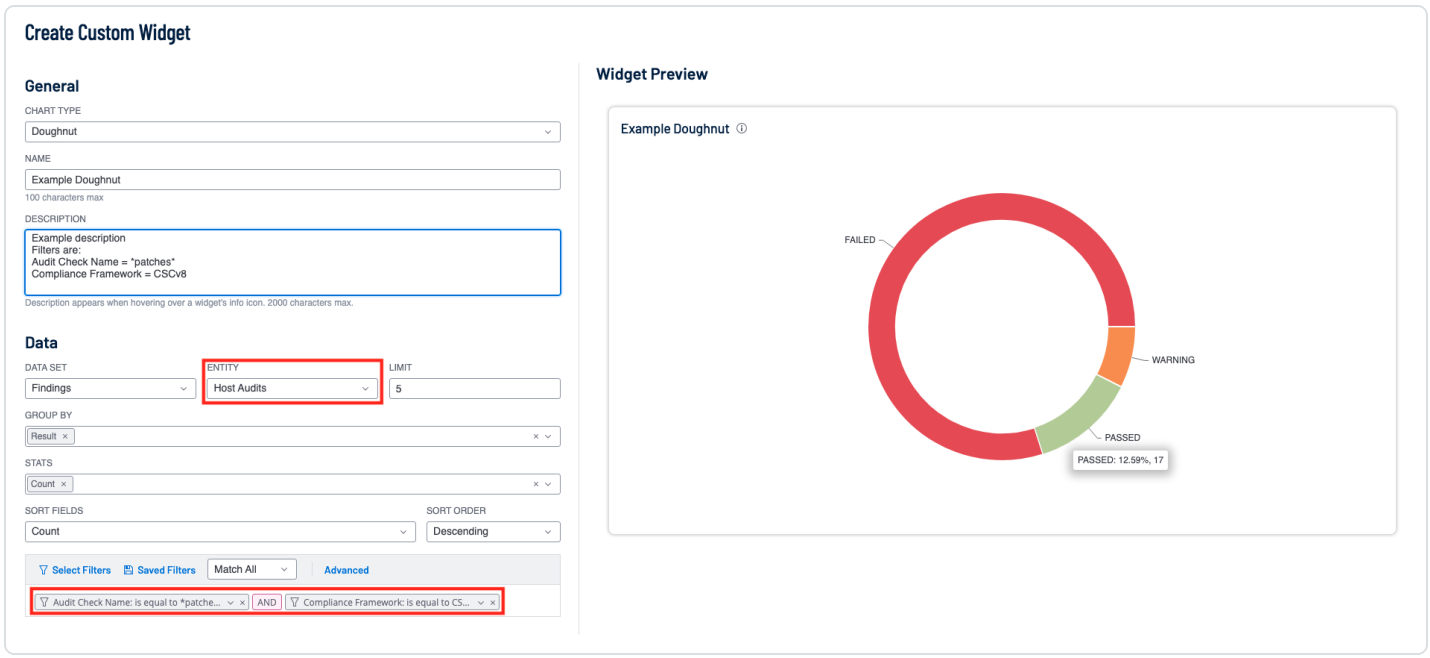
Creating widgets in Tenable Vulnerability Management or components in Tenable Security Center can help a security team visualize the data coming from the compliance scans run. After learning about ways to query the compliance data, creating widgets/components can be beneficial to easily track multiple queries. The widgets/components created can also be used within reports in both Tenable Vulnerability Management and Tenable Security Center. In the subsequent examples, the following filters are used to stay consistent unless otherwise noted: Audit Check Name = *patches* and Compliance Framework = CSCv8 for Tenable Vulnerability Management and, Plugin Name contains patches and Cross Reference = CSCv8|7* for Tenable Security Center. The following Widget/Component types are shown:

- **Pie Chart and Doughnuts**
- **Tables**
- **Bar Charts**

Pie Chart / Doughnut

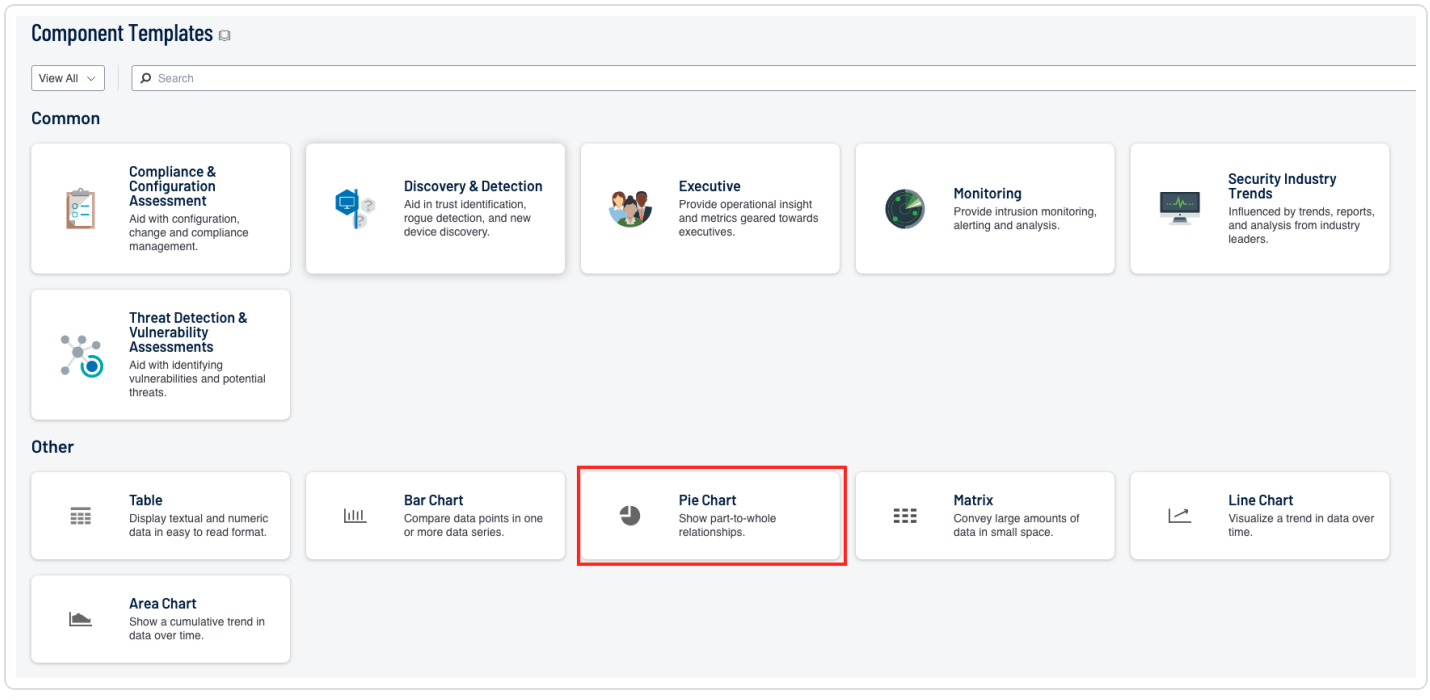
Tenable Vulnerability Management

In Tenable Vulnerability Management the user can create a Doughnut chart by selecting the appropriate Chart Type. One thing to note is that different chart types are supported for different Entities. This means that when first starting to create a custom widget, setting the Entity resets the chart type, as the chosen one may not be available. In the Doughnut Chart example following the user can set the Entity to Host Audits, Chart Type to Doughnut, Group by to Result, Status to Count and Sort Fields to Count. These settings in combination with the Audit Check Name = *patches* and Compliance Framework = CSCv8 filters results in a visualization of the compliance results that include the word patches that are related to the CSCv8 Framework.



Tenable Security Center

In Tenable Security Center the user can create a Pie Chart by selecting the appropriate selection within the "Other" section on the Component Templates page.



To match the example the user can use the "Severity Summary" tool to allow the pie chart to display the different Host Audit result types that match the query. Do note that with this tool the Low and

Critical severities will always show 0% since compliance results can either be Info, Medium, or High Severity.

General

NAME * Testing

DESCRIPTION Example Bar Chart

SCHEDULE * Every day at 11:00 -04:00

Data

TYPE Vulnerability

QUERY *Select a Query*

SOURCE Cumulative

TOOL IP Summary

FILTERS

Cross References	= CSCv8I7*
Plugin Name	Contains patches

+ Add Filter

Display

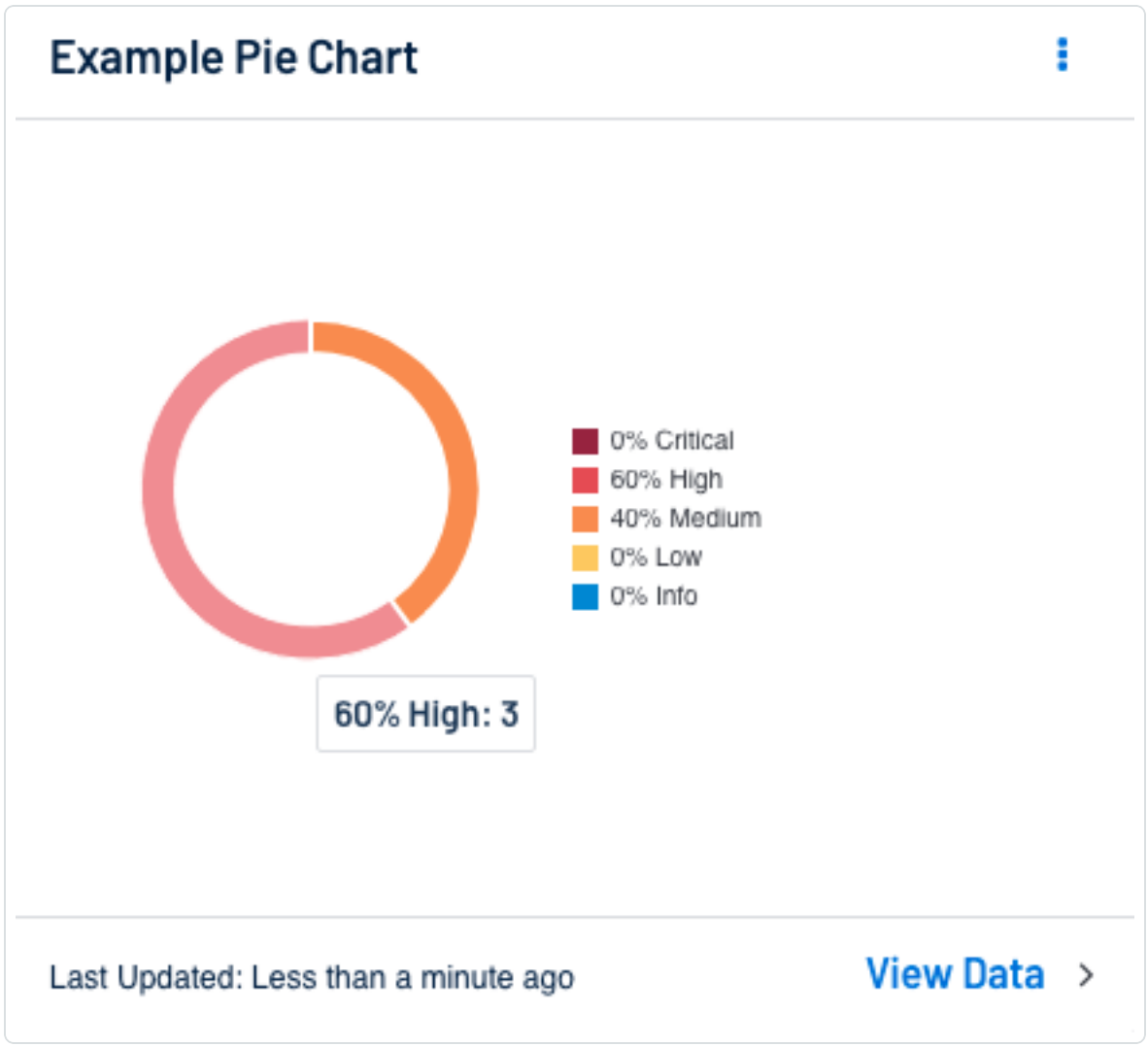
RESULTS DISPLAYED 10

SORT COLUMN High

SORT DIRECTION Descending

DISPLAY COLUMNS

- [ ] Select All
- [ ] Score
- [x] Info
- [ ] Low
- [x] Medium
- [x] High

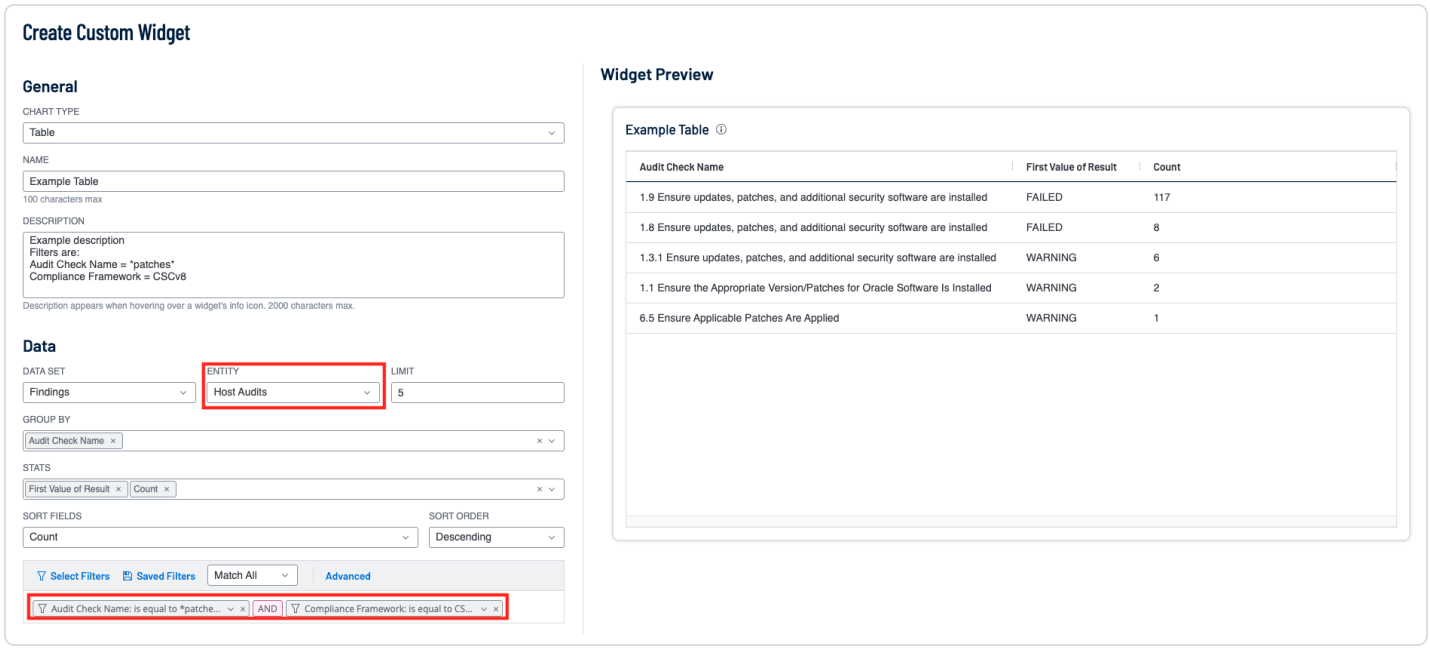


Table

Tenable Vulnerability Management

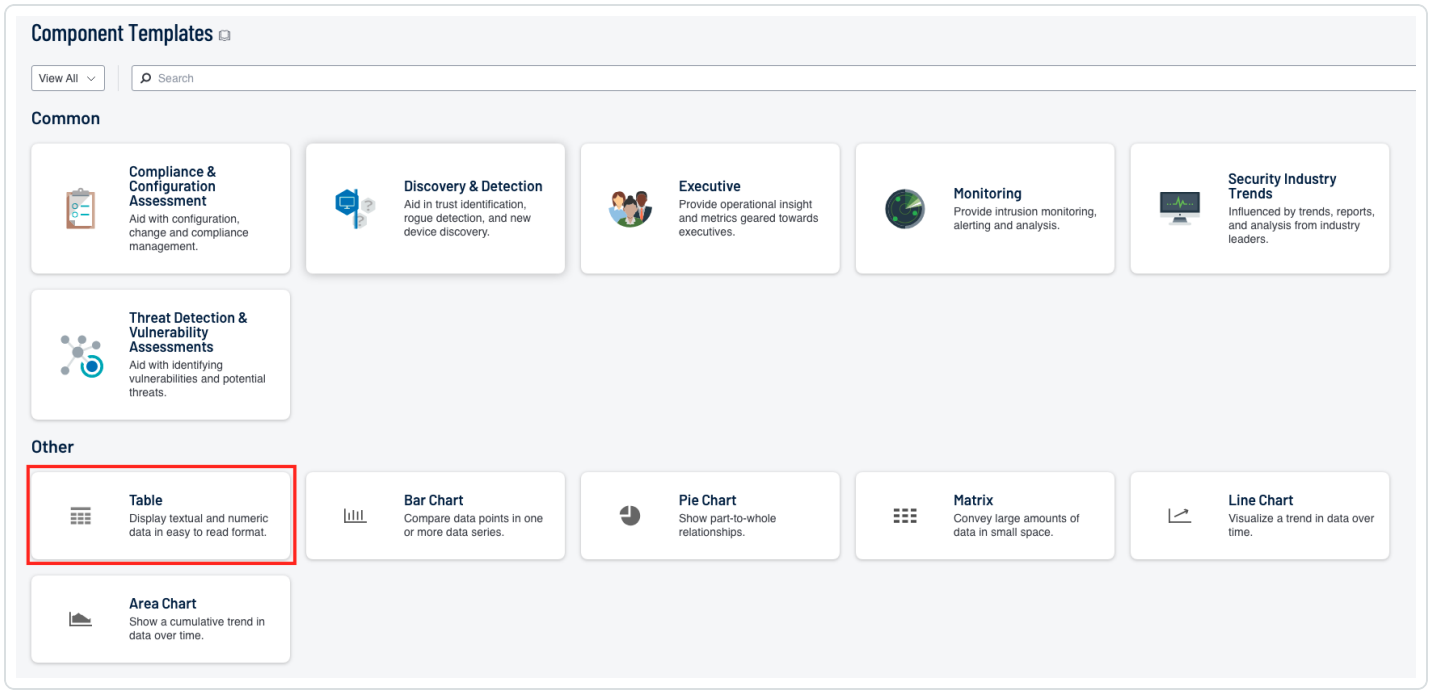
Tables in Tenable Vulnerability Management can be a quick way to visualize more detail in a condensed form. With many available columns available to use (the specific columns available are determined by the entity type), the user is able to quickly identify the most commonly failed checks in their organization. In the following example, using the same filters as the previous Tenable Vulnerability Management example, the widget displays the Audit Check which was run the most because the widget is sorted by count. The widget also displays the result of the first value of Results, this means the widget is only looking at the first value seen and prints it out. This can lead to a misinterpretation of the data as it may appear that there are 117 FAILED results when in reality

it could be only one result failed and the rest passed. To rectify this, the user can add a Results filter to ensure only one result type is included in the Count column.



Tenable Security Center

Tables in Tenable Security Center can provide the same level of condensed detail that they can in Tenable Vulnerability management. Though in Tenable Security Center the determining factor on which columns can be used is the Tool used. The Table chart type can be selected via the Component Template page under the “Other” Section.



The following example shows the Vulnerability Summary tool to display the name of the audit checks run along with the severity and total number seen. This widget displays all result types seen, so the user can add the severity filter to see only a certain type of result. With this widget the total number represents the total number of specified plugin names and severity seen. This means that unlike in Tenable Vulnerability Management where the column is for the first value, Tenable Security Center separates the result types.

General

NAME *: Testing

DESCRIPTION: Example Bar Chart

SCHEDULE *: Every day at 11:00 -04:00

Data

TYPE: Vulnerability

QUERY: *Select a Query*

SOURCE: Cumulative

TOOL: IP Summary

FILTERS

Cross References	= CSCv8I7*
Plugin Name	Contains patches

+ Add Filter

Display

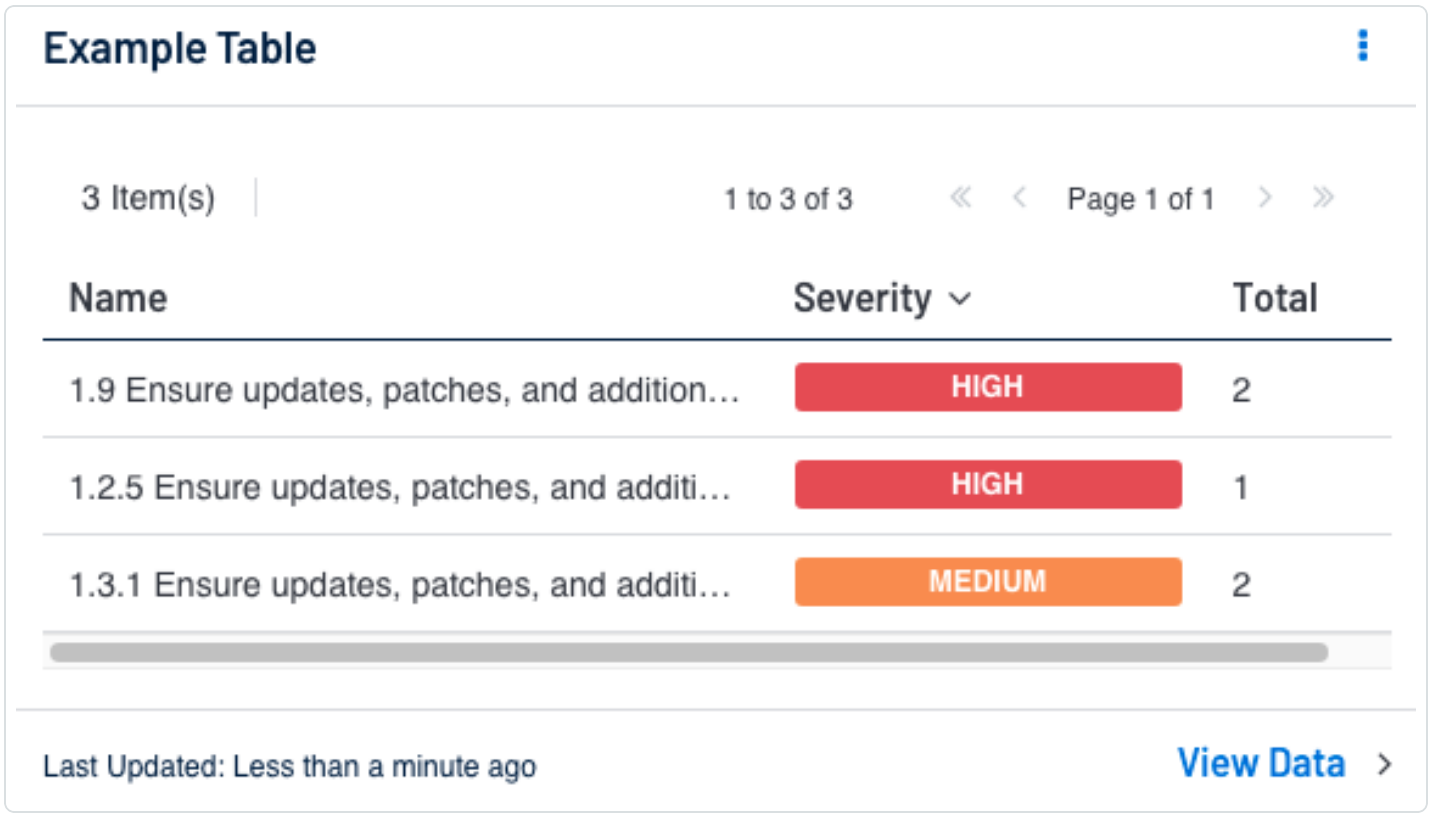
RESULTS DISPLAYED: 10

SORT COLUMN: High

SORT DIRECTION: Descending

DISPLAY COLUMNS:

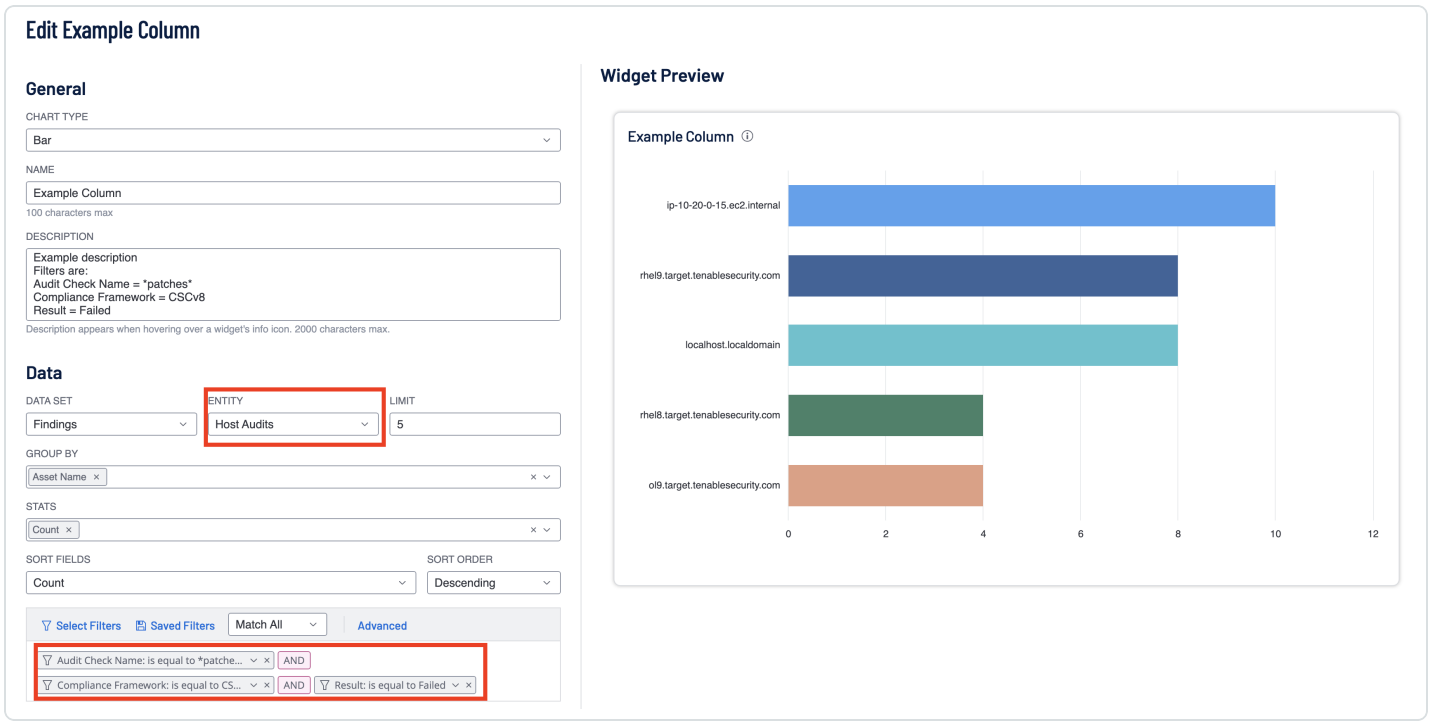
- [ ] Select All
- [ ] Score
- [x] Info
- [ ] Low
- [x] Medium
- [x] High



Bar / Column

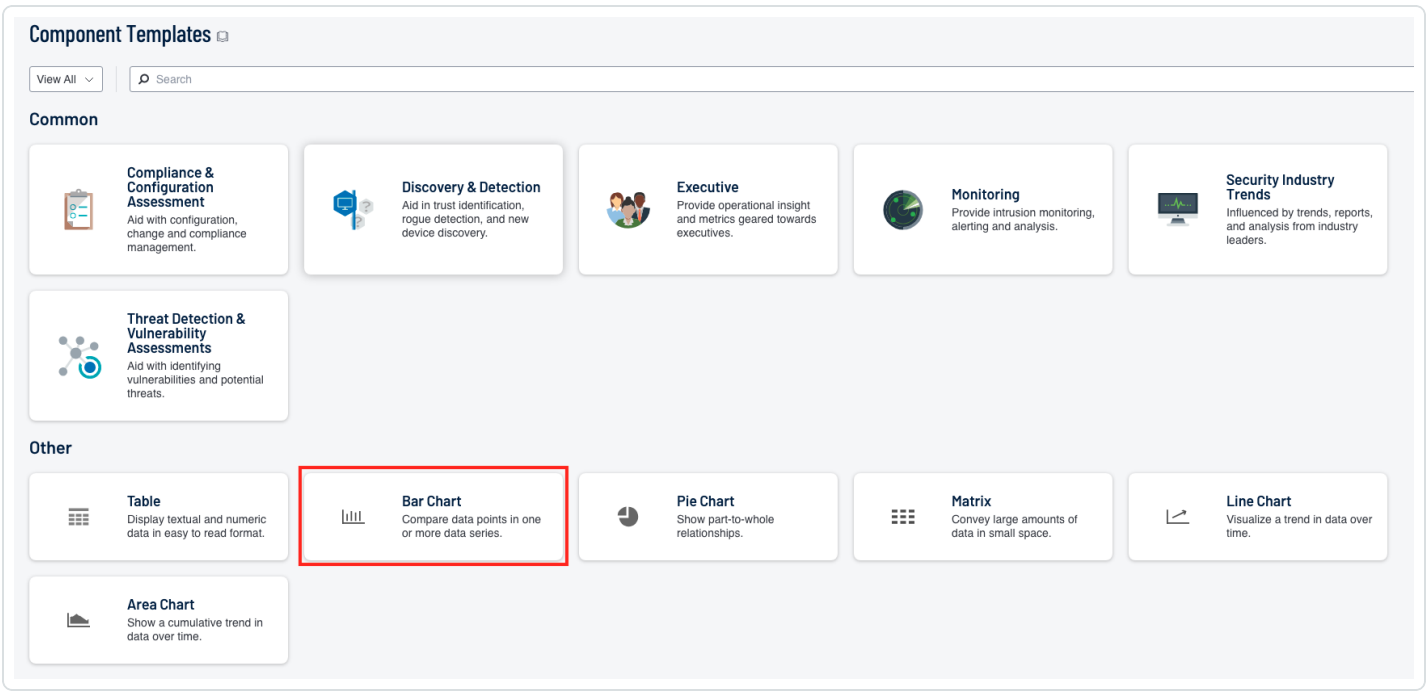
Tenable Vulnerability Management

Tenable Vulnerability Management has two available bar-like chart types for Host Audit Entity: Bar and Column. These two chart types function the same way with the only difference being the orientation of the bar; bar charts are horizontal and columns are vertical. The following example groups the results by Asset Name and sorts by count. This configuration of the widget allows the user to see which asset has the most failed audit checks which match the filters used.



Tenable Vulnerability Management

Tenable Vulnerability Management has two available bar-like chart types for Host Audit Entity: Bar and Column. These two chart types function the same way with the only difference being the orientation of the bar; bar charts are horizontal and columns are vertical. The following example groups the results by Asset Name and sorts by count. This configuration of the widget allows the user to see which asset has the most failed audit checks which match the filters used.



This example uses the IP summary tool to better match the example given above and to display the counts of audit checks separated by assets. The Columns chosen in the widget are Info, Medium, and High to include all possible result types in Compliance scans: Passed, Manual, and Failed.

General

NAME * Testing

DESCRIPTION Example Bar Chart

SCHEDULE * Every day at 11:00 -04:00

Data

TYPE Vulnerability

QUERY *Select a Query*

SOURCE Cumulative

TOOL IP Summary

FILTERS

Cross References	= CSCv8I7*
Plugin Name	Contains patches

+ Add Filter

Display

RESULTS DISPLAYED 10

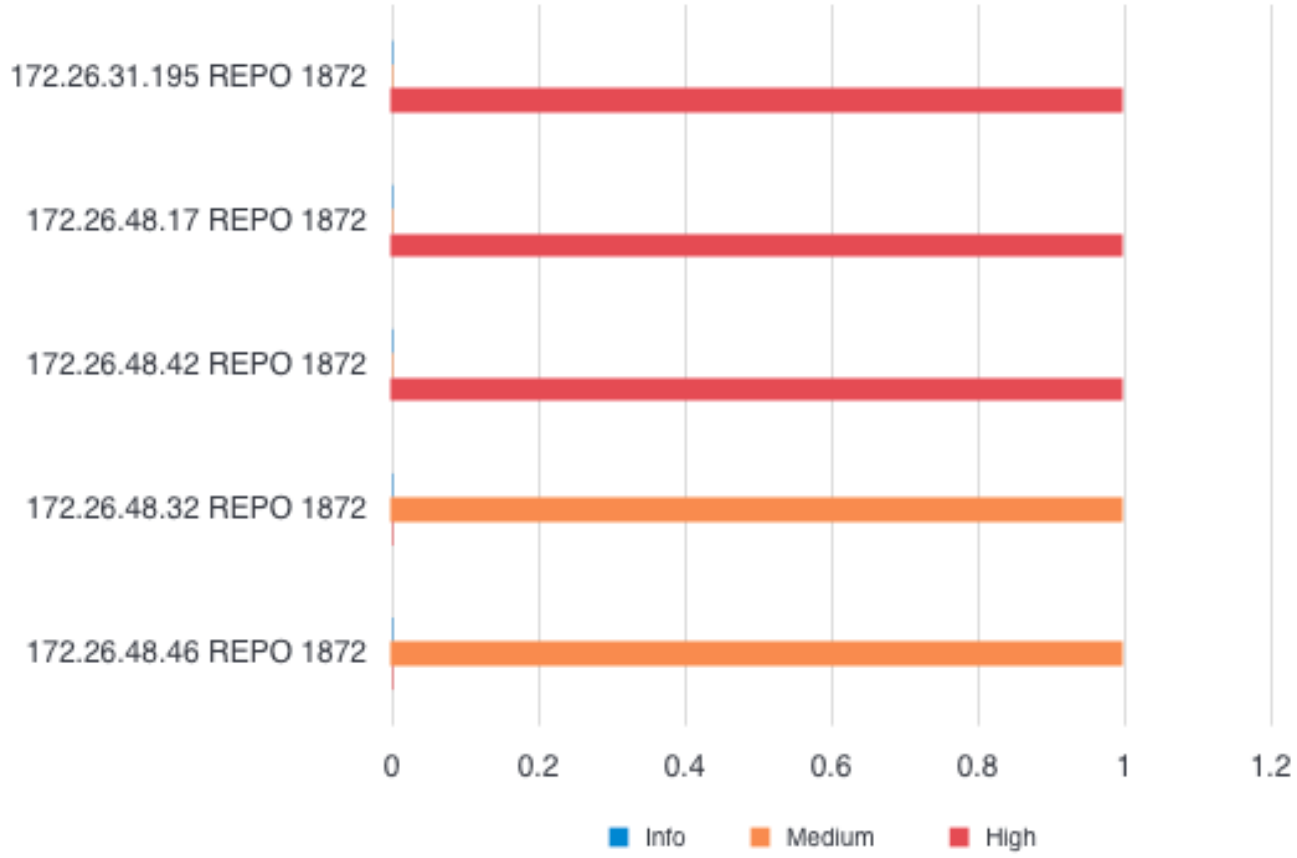
SORT COLUMN High

SORT DIRECTION Descending

DISPLAY COLUMNS

- [ ] Select All
- [ ] Score
- [x] Info
- [ ] Low
- [x] Medium
- [x] High

Testing



Last Updated: 3 minutes ago

View Data >

Learn More

Tenable

- Plugins Search
- Tenable Vulnerability Management Findings Filters
- Tenable Security Center (6.3) Vulnerability Analysis Filter Components
- Audits Documentation
- Compliance Checks Reference
- Tenable Cyber Exposure Study – Host Audit Data

Compliance References

- CIS CSCv8 - CIS Critical Security Controls Version 8
- 800-171 - NIST SP 800-171
- CSF - NIST Cyber Security Framework (CSF)
- ISO/IEC 27001
- 800-53 - NIST SP 800-53