Tenable Cyber Exposure Study - Application Software Security

Last Revised: February 28, 2024

Table of Contents

Overview

Applications enable users to interface and manipulate data in a consistent manner and often have the ability to interface with system functions and critical databases to add or modify data. Attackers can leverage flaws in applications to bypass access controls. Web applications, which are internet-facing, are a particular security concern since they present a global attack vector. This document describes how Tenable customers can leverage Tenable solutions to ensure application security processes are aligned with common industry-standard security practices.

How Tenable Can Help

Leveraging Tenable Vulnerability Management (formerly Tenable.io) and Tenable Web App Scanning (formerly Tenable.io Web Application Scanning) solutions enables organizations to close attack paths, making the organization a more difficult target to attack. Web application scanning is also available as an on-premises solution, seamlessly integrated into Tenable Security Center. This empowers all customers, regardless of deployment preference, to enhance their security posture and protect against web app vulnerabilities. Tenable solutions provide organizations the data needed to identify and evaluate exposures in the environment. Tenable Vulnerability management provides a platform approach to a risk-based view of the organization's information technology, security and compliance posture. Tenable Web App Scanning, a component of Tenable Vulnerability Management, helps security teams understand the page structure and layout of web applications. Tenable Security Center is an on-premises solution that provides a risk-based view of the organization's information technology, security and compliance posture.

Application security is the process used to enhance the security of application code to protect against threats during all phases of development. An effective application security program goes beyond just evaluating code and includes all the security measures at the application level to prevent data loss, unauthorized access, or modification. The application security process encompasses not only the application design and development phases for custom applications, but most importantly the approaches to protect applications after they are deployed, regardless of whether they are commercial products or developed in-house.

Applications are the components that drive business objectives, are often available over internal and external networks and connected to the cloud. Often, device security comes in second place to developing features to perform a required business function. Attackers typically do not gain access to sensitive data by physically attacking hardware. Most data breaches occur because a particular application or operating system had a weakness or vulnerability that allowed an attacker to gain access to the device.

Application security includes anything that identifies or minimizes security vulnerabilities to the application, including hardware, software, and any procedures such as regular testing. Web application security is of special importance since web applications are designed to be available to anyone on the networks they are connected to, which usually includes the entire internet.

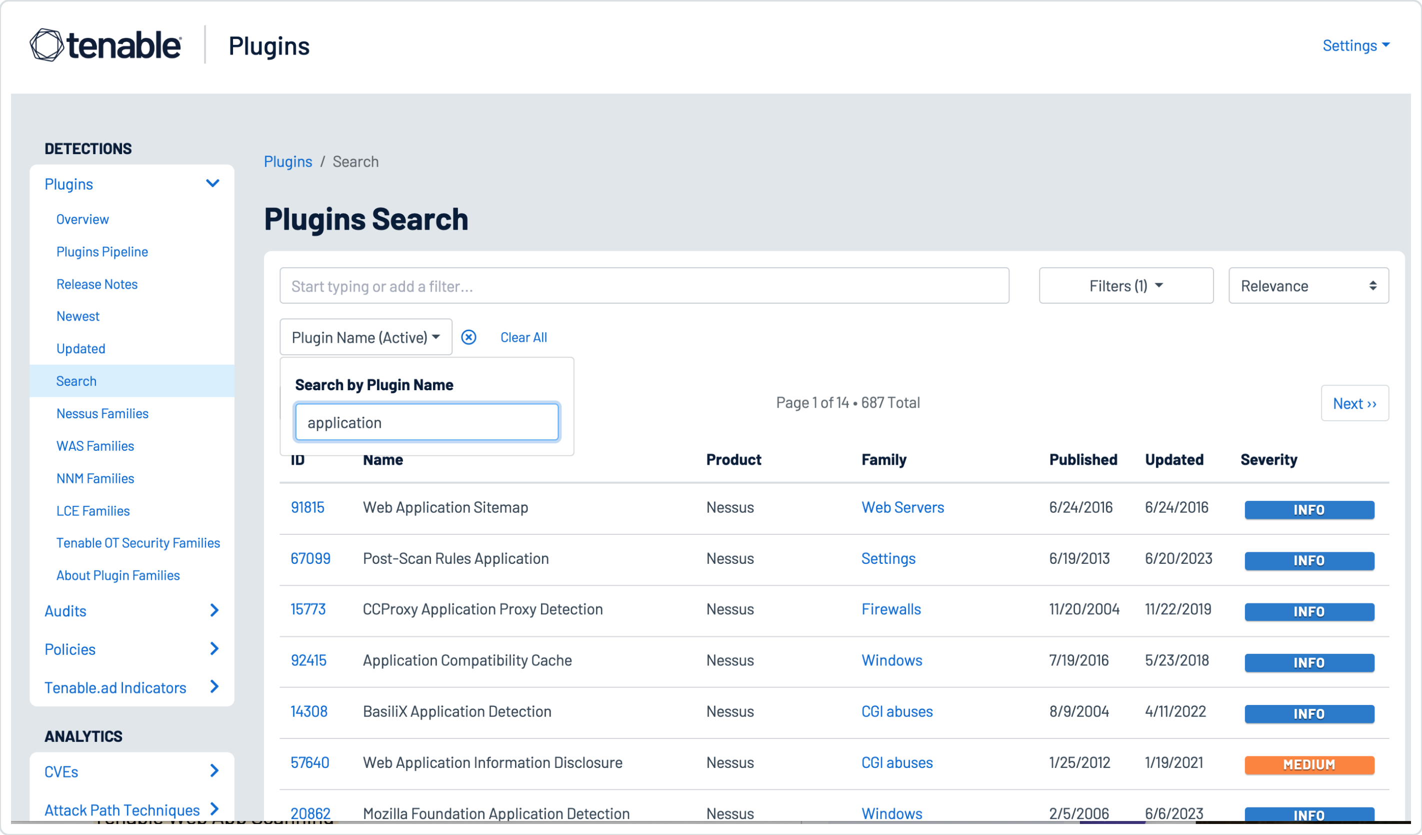
This guide provides a detailed approach to application security and includes information to address key focus areas such as:

- **Vulnerability Management** – The identification of software inventory, trusted applications/components, identification of unsupported/end-of-life/out-of-date software, and the prioritization and remediation tracking of these vulnerabilities.
- **Ports and Services** – The identification of ports and services.
- **ID Management** – The identification of privileged accounts, user access, default accounts, and the use of proper encryption.
- **Server/Application Hardening** – The audit of the configuration of the underlying operating system and applications to defined and established standards, such as the CIS Benchmarks.

Vulnerability Management

Tenable Vulnerability Management and Tenable Security Center enable security teams to focus on the vulnerabilities and assets, which matter most to the organization, while deprioritizing the vulnerabilities that attackers are unlikely to ever exploit. Regular testing, including vulnerability assessments help identify and remediate potential vulnerabilities in software and web applications.

As information about new vulnerabilities is discovered and released into the general public domain, Tenable Research designs plugins to detect and evaluate the risks posed by these vulnerabilities. The plugins contain vulnerability information, a simplified set of remediation actions and the algorithm to test for the presence of security exposures. Tenable Research has published many plugins, which detect application issues, as shown in the following image:



Plugins Search

Search by Plugin Name: application

Page 1 of 14 • 687 Total

ID	Name	Product	Family	Published	Updated	Severity
91815	Web Application Sitemap	Nessus	Web Servers	6/24/2016	6/24/2016	INFO
67099	Post-Scan Rules Application	Nessus	Settings	6/19/2013	6/20/2023	INFO
15773	CCProxy Application Proxy Detection	Nessus	Firewalls	11/20/2004	11/22/2019	INFO
92415	Application Compatibility Cache	Nessus	Windows	7/19/2016	5/23/2018	INFO
14308	BasiliX Application Detection	Nessus	CGI abuses	8/9/2004	4/11/2022	INFO
57640	Web Application Information Disclosure	Nessus	CGI abuses	1/25/2012	1/19/2021	MEDIUM
20862	Mozilla Foundation Application Detection	Nessus	Windows	2/5/2006	6/6/2023	INFO

In addition, the Tenable OWASP report and dashboard (for Tenable Vulnerability Management) and the OWASP report and dashboard (for Tenable Security Center) provides organizations the ability to monitor web applications by identifying the top 10 most critical web application security risks as described in the OWASP Top 10 Application Security Risks document.

Tenable Web App Scanning

Tenable Web App Scanning is a dynamic application security testing application which crawls a running web application through the front end 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.

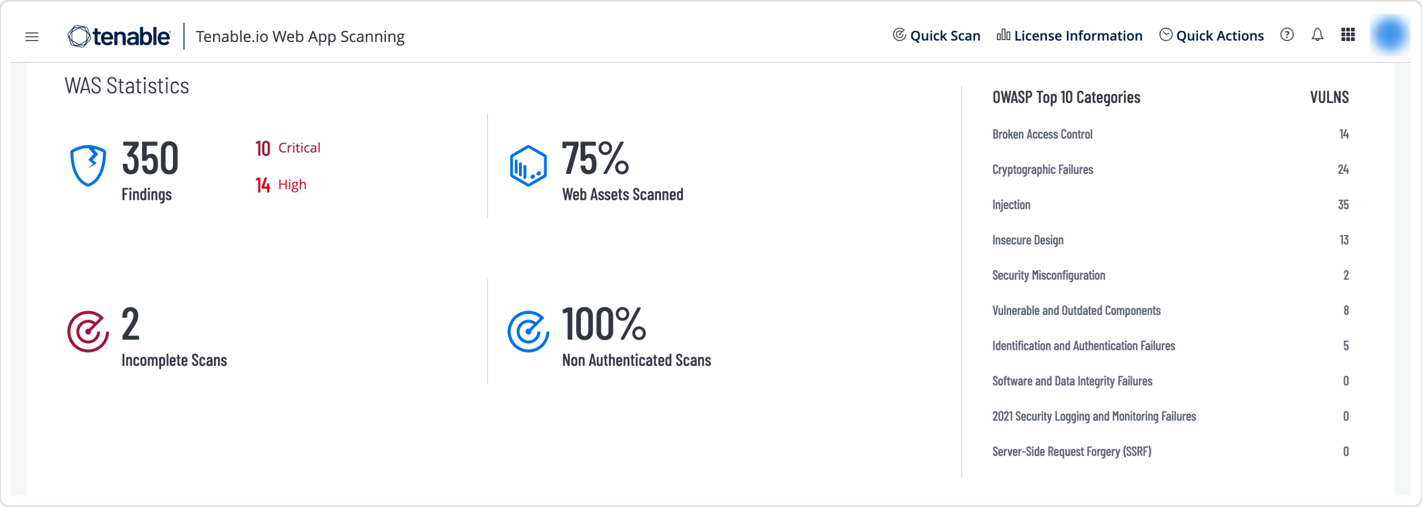
Web application scanning is of critical importance because users typically access these applications from a browser over the internet. Web applications exist on remote servers or in cloud environments, and data is transmitted over public networks. Web application security is a critical aspect to ensure 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.



WAS Statistics

350 Findings

10 Critical

14 High

75% Web Assets Scanned

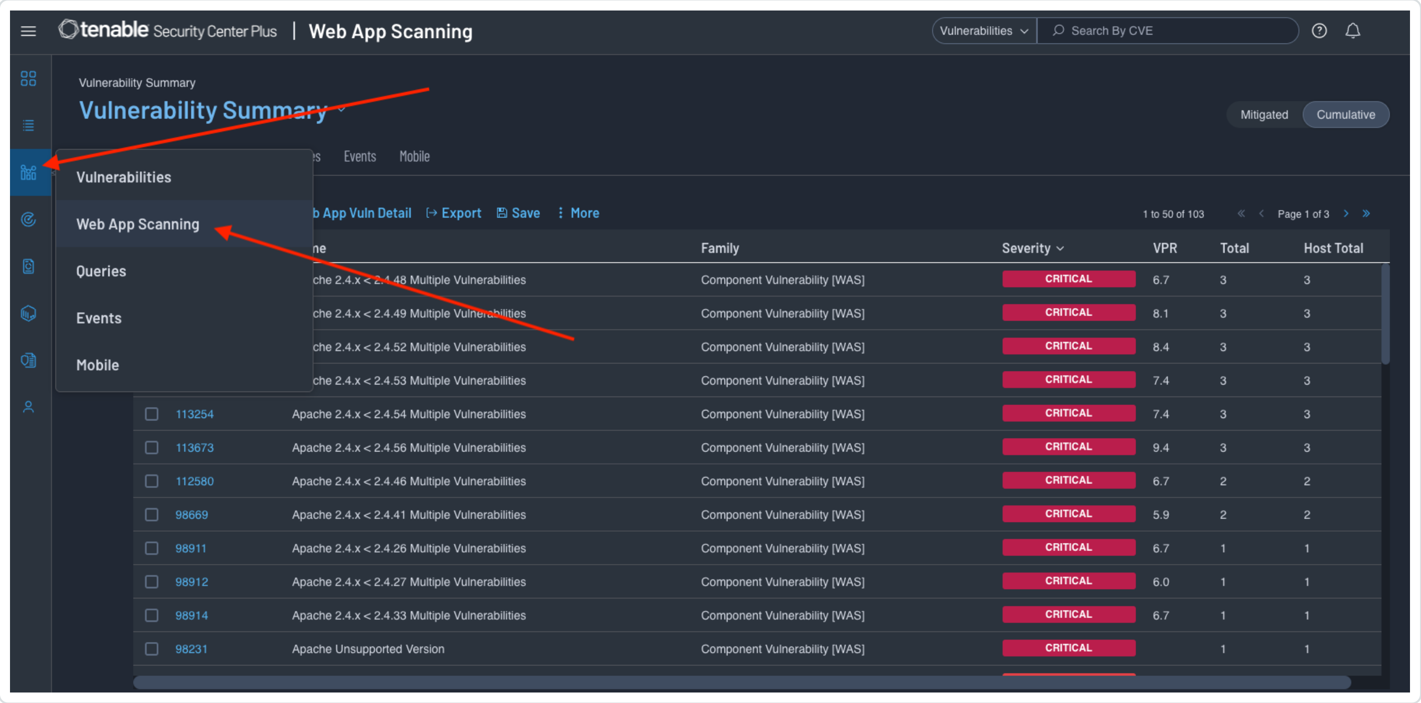
2 Incomplete Scans

100% Non Authenticated Scans

OWASP Top 10 Categories	VULNS
Broken Access Control	14
Cryptographic Failures	24
Injection	35
Insecure Design	13
Security Misconfiguration	2
Vulnerable and Outdated Components	8
Identification and Authentication Failures	5
Software and Data Integrity Failures	0
2021 Security Logging and Monitoring Failures	0
Server-Side Request Forgery (SSRF)	0

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.

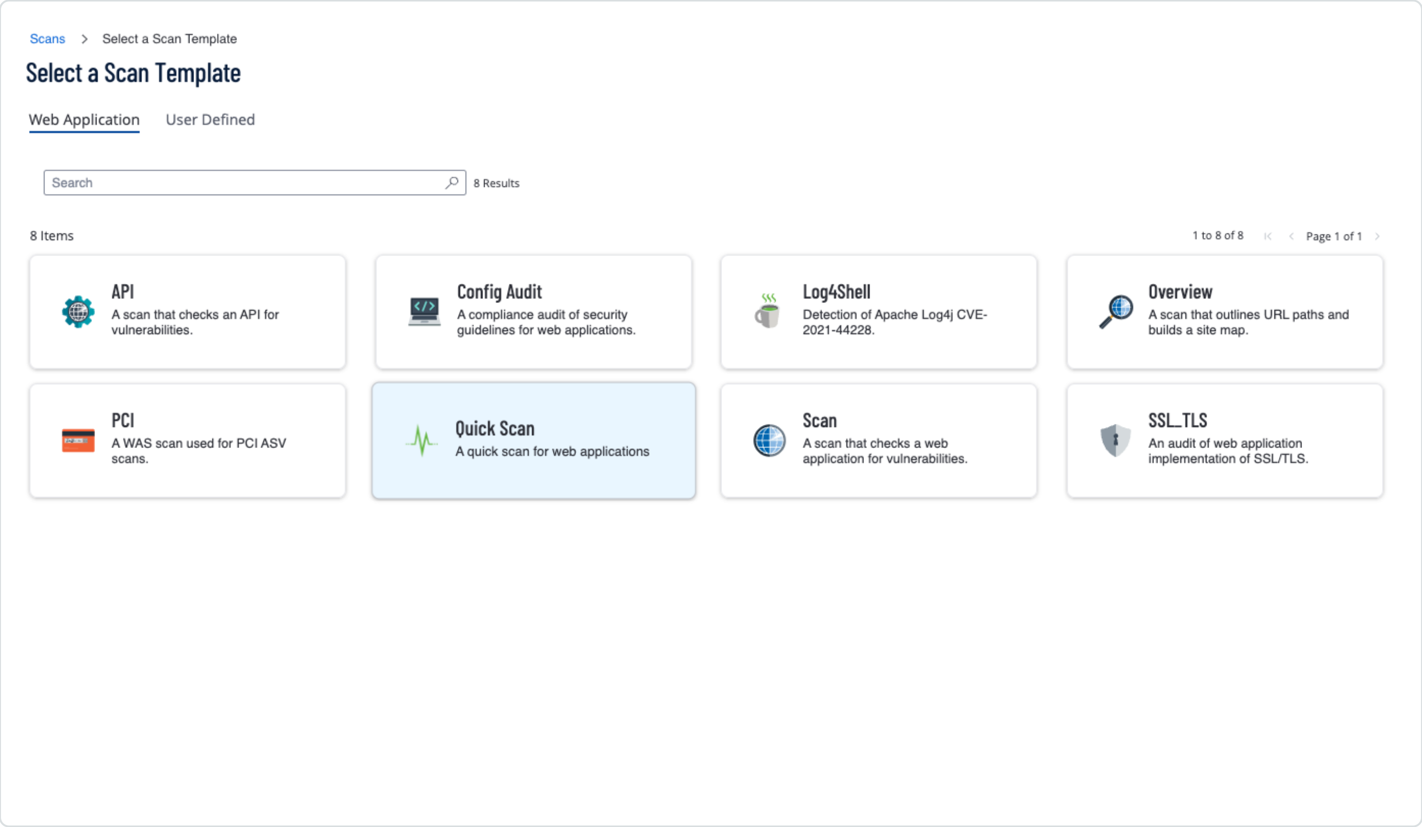
Tenable Web App Scanning vulnerability data within Tenable.sc is available by selecting the Analysis tab, then selecting Web App Scanning to view the web application vulnerability analysis tab.



		ne	Family	Severity	VPR	Total	Host Total
		che 2.4.x < 2.4.48 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	6.7	3	3
		che 2.4.x < 2.4.49 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	8.1	3	3
		che 2.4.x < 2.4.52 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	8.4	3	3
		che 2.4.x < 2.4.53 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	7.4	3	3
□	113254	Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	7.4	3	3
□	113673	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	9.4	3	3
□	112580	Apache 2.4.x < 2.4.46 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	6.7	2	2
□	98669	Apache 2.4.x < 2.4.41 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	5.9	2	2
□	98911	Apache 2.4.x < 2.4.26 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	6.7	1	1
□	98912	Apache 2.4.x < 2.4.27 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	6.0	1	1
□	98914	Apache 2.4.x < 2.4.33 Multiple Vulnerabilities	Component Vulnerability [WAS]	CRITICAL	6.7	1	1
□	98231	Apache Unsupported Version	Component Vulnerability [WAS]	CRITICAL		1	1

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 expire SSL/TLS Certificates.
- Identification of misconfigured web servers.



Select a Scan Template

API
A scan that checks an API for vulnerabilities.

Config Audit
A compliance audit of security guidelines for web applications.

Log4Shell
Detection of Apache Log4j CVE-2021-44228.

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

PCI
A WAS scan used for PCI ASV scans.

Quick Scan
A quick scan for web applications

Scan
A scan that checks a web application for vulnerabilities.

SSL_TLS
An audit of web application implementation of SSL/TLS.

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 that 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).

Tenable Identity Exposure

Many operating systems provide effective critical security functions and mechanisms to applications which control identification, authentication, and authorization to applications. The three key elements of Identity Management, as related to application security are defined as follows:

The three key elements of Identity Management, as related to application security are defined as follows:

- **Identification:** The process of establishing a unique identity for each user or entity within the system, such as usernames, email addresses, or other IDs that uniquely identify individuals.
- **Authentication:** The process of verifying the identity of a user or entity. This ensures that the person or system trying to access the resources are who they claim to be.
- **Authorization:** Once an identity has been authenticated, authorization determines what resources or actions are allowed to be accessed.

These elements and associated policies, processes, and tools play a crucial role to help organize, secure, and manage digital identities in securing web applications.

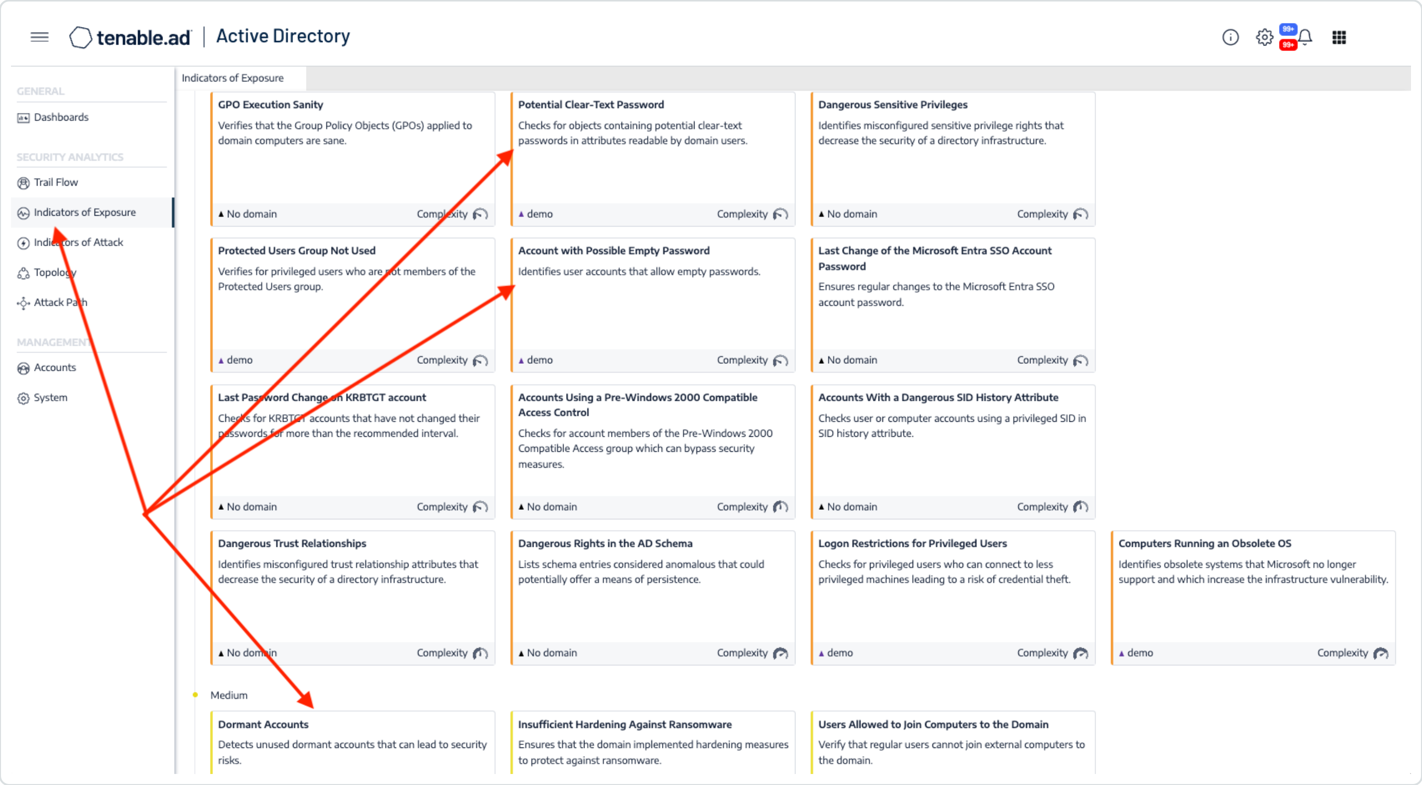
Identity Management

Tenable Identity Exposure (formerly Tenable.ad) provides information about the organization's Active Directory environment in an intuitive dashboard, which monitors Active Directory in real-time, enabling organizations to identify at a glance the most critical vulnerabilities and recommended courses of remediation.

Some of the Application Security compliance requirements Tenable solutions address may include:

- Identify all accounts in the environment.
- Ensure all active accounts are authorized.
- Ensure all accounts are configured to use strong authentication controls.
- Delete or disable dormant and default accounts.
- Restrict privileged access to only authorized users.
- Ensure group access is appropriately assigned.
- Understand configuration exposures, such as dangerous permissions.

Indicators of Exposure, a feature of Tenable Identity Exposure, provides an overview of critical, high, medium, and low risk exposures identified across the organization’s domains. In this example, several indicators are quickly identified, such as potential clear text passwords, dormant accounts, and accounts with no passwords.



GPO Execution Sanity
Verifies that the Group Policy Objects (GPOs) applied to domain computers are sane.
No domain — Complexity

Potential Clear-Text Password
Checks for objects containing potential clear-text passwords in attributes readable by domain users.
demo — Complexity

Dangerous Sensitive Privileges
Identifies misconfigured sensitive privilege rights that decrease the security of a directory infrastructure.
No domain — Complexity

Protected Users Group Not Used
Verifies for privileged users who are not members of the Protected Users group.
demo — Complexity

Account with Possible Empty Password
Identifies user accounts that allow empty passwords.
demo — Complexity

Last Change of the Microsoft Entra SSO Account Password
Ensures regular changes to the Microsoft Entra SSO account password.
No domain — Complexity

Last Password Change on KRBTGT account
Checks for KRBTGT accounts that have not changed their passwords for more than the recommended interval.
No domain — Complexity

Accounts Using a Pre-Windows 2000 Compatible Access Control
Checks for account members of the Pre-Windows 2000 Compatible Access group which can bypass security measures.
No domain — Complexity

Accounts With a Dangerous SID History Attribute
Checks user or computer accounts using a privileged SID in SID history attribute.
No domain — Complexity

Dangerous Trust Relationships
Identifies misconfigured trust relationship attributes that decrease the security of a directory infrastructure.
No domain — Complexity

Dangerous Rights in the AD Schema
Lists schema entries considered anomalous that could potentially offer a means of persistence.
No domain — Complexity

Logon Restrictions for Privileged Users
Checks for privileged users who can connect to less privileged machines leading to a risk of credential theft.
demo — Complexity

Computers Running an Obsolete OS
Identifies obsolete systems that Microsoft no longer support and which increase the infrastructure vulnerability.
demo — Complexity

Dormant Accounts
Detects unused dormant accounts that can lead to security risks.

Insufficient Hardening Against Ransomware
Ensures that the domain implemented hardening measures to protect against ransomware.

Users Allowed to Join Computers to the Domain
Verify that regular users cannot join external computers to the domain.

For information on user account exposures, refer to the Tenable Cyber Exposure Study: Identity and Access Management document.

Software Inventory

Software inventory refers to the process of cataloging and documenting all the software applications installed on the systems within the organization. Establishing an inventory of all software and applications running in the environment is not only a fundamental step to secure the organization, but a key step in application software security. Identifying software usage is necessary to ensure software assets are authorized, appropriately licensed, supported, and have the most recent security fixes applied. A current software inventory also helps demonstrate compliance with regulatory controls and Service Level Agreements (SLAs) for software used in the environment.

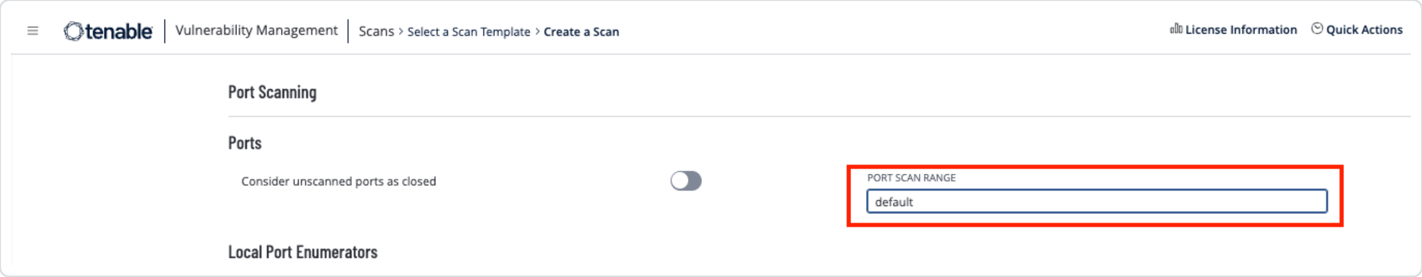
Performing regular software inventory checks also identifies unnecessary software running in the environment, which increases the attack surface without providing a business advantage. In addition, running unnecessary software creates overhead and an inefficient runtime environment. Finally, a software inventory helps identify applications using components with known vulnerabilities that may undermine application defenses and enable a range of possible attacks and impacts. For more information on software inventory see the Tenable Cyber Exposure Study, Establishing a Software Inventory.

Detecting Ports and Services

Open ports can pose a security risk if they are associated with services that have known vulnerabilities, or if they are unintentionally exposed to the internet. Ports and services must be regularly audited and monitored to ensure only necessary services are accessible and they are adequately protected against potential threats. Secure design includes the concept of least privilege and minimizing the attack surface, including the identification of unprotected ports and services. Disable unused and unprotected ports and services to reduce the attack surface and minimize risk.

Detecting Ports

Tenable Nessus does not scan all ports by default. To scan all ports edit the scan policy, under Discovery -> Port Scanning.



Port Scanning

Ports

Consider unscanned ports as closed

PORT SCAN RANGE

default

Local Port Enumerators

The port scan range can be set to an explicit value, range, combination of both, or default. When set using the keyword 'default,' the scanner scans approximately 4,790 common ports. This can be set to ‘all’ to scan all 65,536 ports (including port 0). The list of ports can be found in the nessus-services file on the Tenable Nessus scanner. This list can change over time.

> **Note:** There are risks associated with scanning all ports, as some sensitive devices may react abnormally. Ensure that you are aware of the devices you are scanning by altering this setting.

Detecting Services

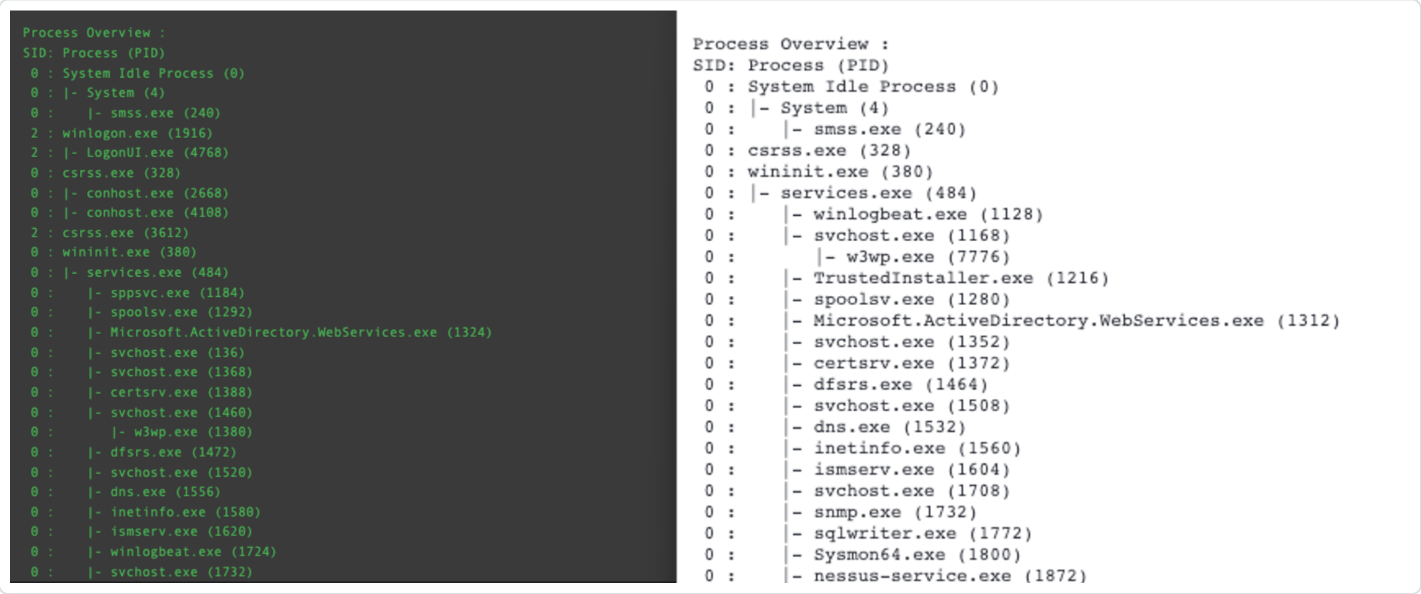
Tenable Vulnerability Management and Tenable Security Center include plugins that detect running services and process information. The information from these plugins can display unregistered software running on the system that is not shown in the registry. The following plugins provide visibility into services that may appear only in running processes rather than in installed software packages.

- 58452 - Microsoft Windows Startup Software Enumeration.
- 70329 - Microsoft Windows Process Information.
- 70330 - Microsoft Windows Process Unique Process Name
- 70331 - Microsoft Windows Process Module Information.
- 70767 - Reputation of Windows Executables: Known Process(es).
- 70768 - Reputation of Windows Executables: Unknown Process(es).

- 70943 - Reputation of Windows Executables: Never seen process(es).
- 110483 - Unix/Linux Running Processes Information

A filter can also be applied using Plugin Family: Service Detection.

The following displayed sample output for plugin 70329 shows a "w3wp" process that could be suspicious. Output such as this can be taken from this plugin and used in a further investigative search using the text with the Plugin Output (Vulnerability Text) or CPE filter.

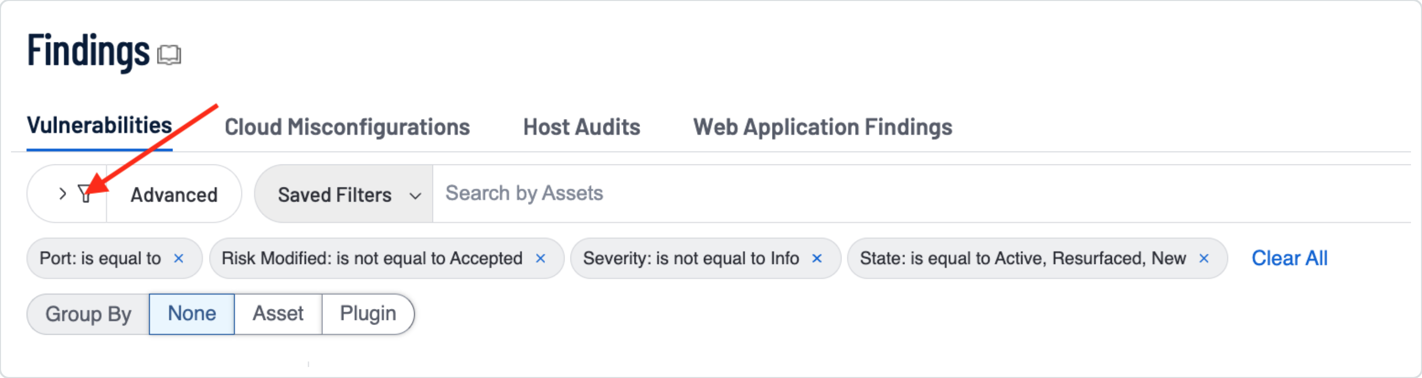


```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- smss.exe (240)
 2 : winlogon.exe (1916)
 2 : |- LogonUI.exe (4768)
 0 : csrss.exe (328)
 0 : |- conhost.exe (2668)
 0 : |- conhost.exe (4108)
 2 : csrss.exe (3612)
 0 : wininit.exe (380)
 0 : |- services.exe (484)
 0 :    |- sppsvc.exe (1184)
 0 :    |- spoolsv.exe (1292)
 0 :    |- Microsoft.ActiveDirectory.WebServices.exe (1324)
 0 :    |- svchost.exe (136)
 0 :    |- svchost.exe (1368)
 0 :    |- certsrv.exe (1388)
 0 :    |- svchost.exe (1460)
 0 :       |- w3wp.exe (1380)
 0 :    |- dfsrs.exe (1472)
 0 :    |- svchost.exe (1520)
 0 :    |- dns.exe (1556)
 0 :    |- inetinfo.exe (1580)
 0 :    |- ismserv.exe (1620)
 0 :    |- winlogbeat.exe (1724)
 0 :    |- svchost.exe (1732)
```

```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- smss.exe (240)
 0 : csrss.exe (328)
 0 : wininit.exe (380)
 0 : |- services.exe (484)
 0 :    |- winlogbeat.exe (1128)
 0 :    |- svchost.exe (1168)
 0 :       |- w3wp.exe (7776)
 0 :    |- TrustedInstaller.exe (1216)
 0 :    |- spoolsv.exe (1280)
 0 :    |- Microsoft.ActiveDirectory.WebServices.exe (1312)
 0 :    |- svchost.exe (1352)
 0 :    |- certsrv.exe (1372)
 0 :    |- dfsrs.exe (1464)
 0 :    |- svchost.exe (1508)
 0 :    |- dns.exe (1532)
 0 :    |- inetinfo.exe (1560)
 0 :    |- ismserv.exe (1604)
 0 :    |- svchost.exe (1708)
 0 :    |- snmp.exe (1732)
 0 :    |- sqlwriter.exe (1772)
 0 :    |- Sysmon64.exe (1800)
 0 :    |- nessus-service.exe (1872)
```

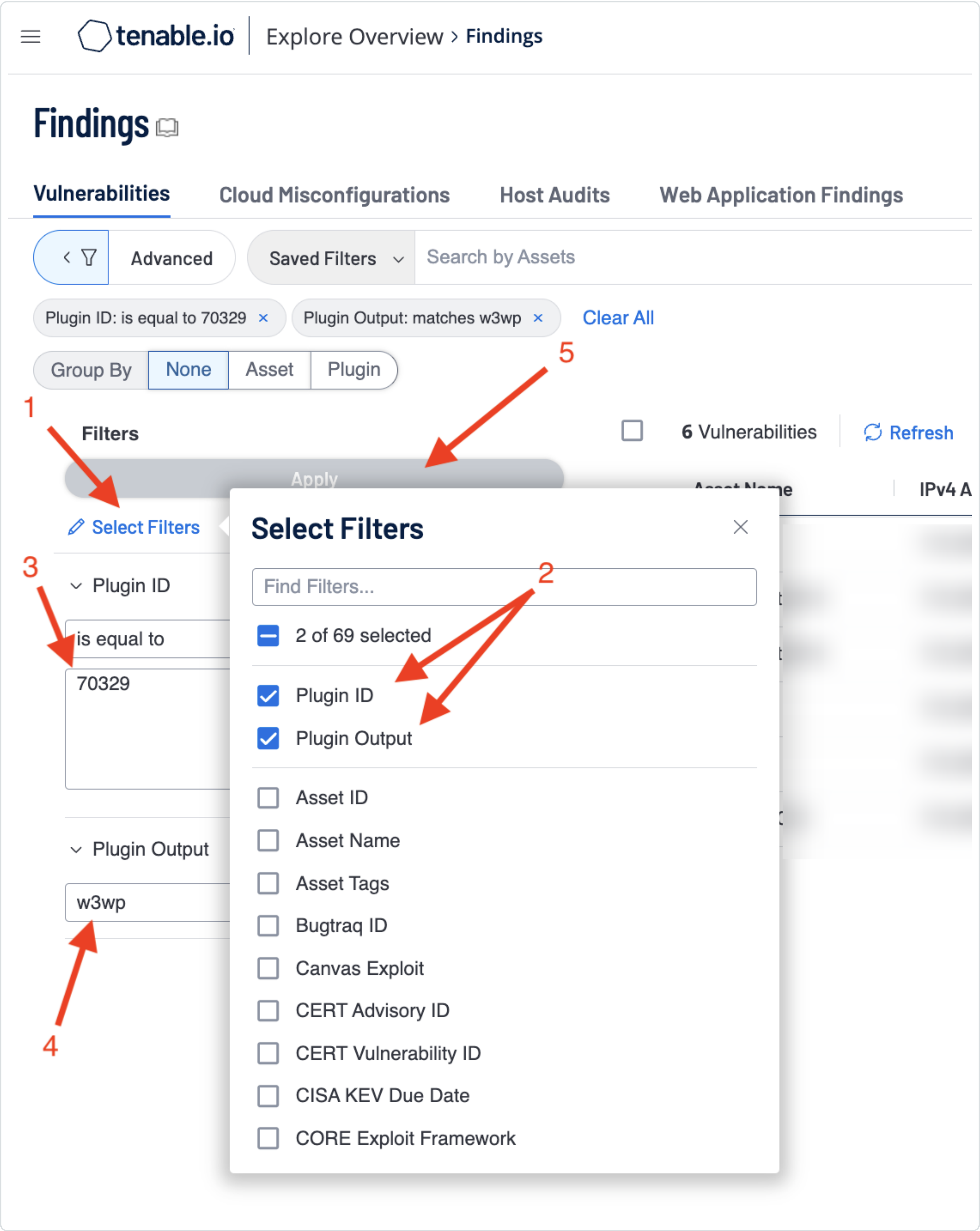
Example Plugin Search

To perform this search in Tenable Vulnerability Management, from the **Findings** page, click on the **Advanced** button and then the filter tab, as shown in the following image:



Findings

An interface to search based on selected criteria is displayed, as shown in the following image. Click on **Select Filters** (**1**) and select the desired filters for the query. In this example, **Plugin ID** and **Plugin Output** (**2**). Deselect any filters, which are not required for the search, by clicking on the check box. Enter the desired Plugin ID for the search (**3**), in this example 70329. Enter the Plugin Output for the search (**4**), in this example "w3wp." Click the Apply button (**5**) to begin the search.



Plugin ID: is equal to 70329 ×

Plugin Output: matches w3wp ×

Select Filters

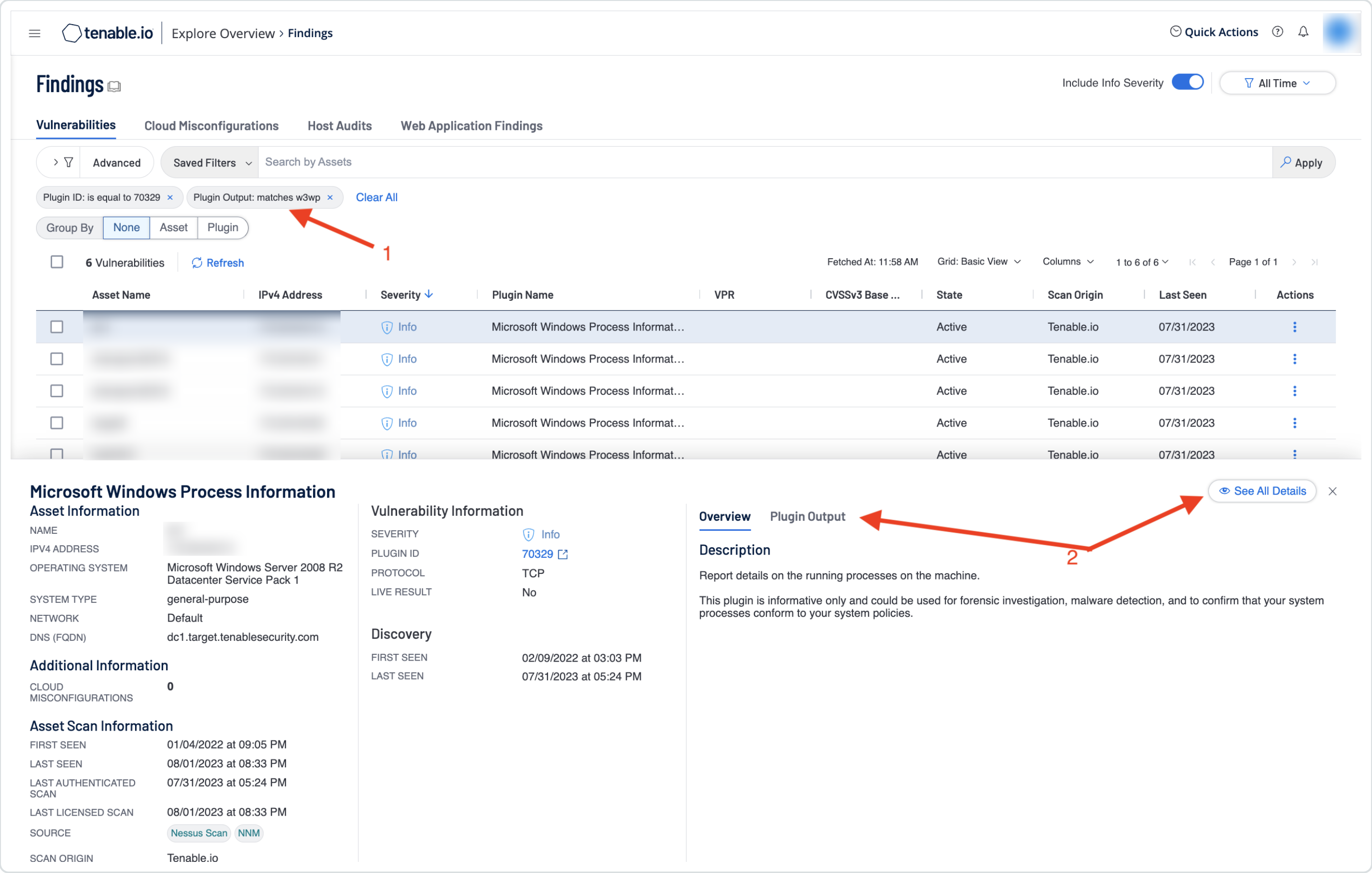
2 of 69 selected

☑ Plugin ID
☑ Plugin Output
□ Asset ID
□ Asset Name
□ Asset Tags
□ Bugtraq ID
□ Canvas Exploit
□ CERT Advisory ID
□ CERT Vulnerability ID
□ CISA KEV Due Date
□ CORE Exploit Framework

Plugin ID
is equal to
70329

Plugin Output
w3wp

The search results page is displayed showing all assets containing the search query filter. For this example, the **Plugin ID** and **Plugin Output** (**1**) are shown. Clicking on a result displays summary information of the results. More details, including the Plugin Output can be found by clicking on either **Plugin Output** or the **See All Details** button (**2**).



Plugin ID: is equal to 70329 ×   Plugin Output: matches w3wp ×

Group By: [✓ None] Asset Plugin

6 Vulnerabilities   Refresh

Fetched At: 11:58 AM   Grid: Basic View   Columns   1 to 6 of 6   Page 1 of 1

Asset Name	IPv4 Address	Severity	Plugin Name	VPR	CVSSv3 Base ...	State	Scan Origin	Last Seen	Actions
[redacted]	[redacted]	Info	Microsoft Windows Process Informat...			Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Info	Microsoft Windows Process Informat...			Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Info	Microsoft Windows Process Informat...			Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Info	Microsoft Windows Process Informat...			Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Info	Microsoft Windows Process Informat...			Active	Tenable.io	07/31/2023	⋮

Microsoft Windows Process Information

Asset Information

NAME [redacted]
IPV4 ADDRESS [redacted]
OPERATING SYSTEM Microsoft Windows Server 2008 R2 Datacenter Service Pack 1
SYSTEM TYPE general-purpose
NETWORK Default
DNS (FQDN) dc1.target.tenablesecurity.com

Additional Information

CLOUD MISCONFIGURATIONS 0

Asset Scan Information

FIRST SEEN 01/04/2022 at 09:05 PM
LAST SEEN 08/01/2023 at 08:33 PM
LAST AUTHENTICATED SCAN 07/31/2023 at 05:24 PM
LAST LICENSED SCAN 08/01/2023 at 08:33 PM
SOURCE Nessus Scan NNM
SCAN ORIGIN Tenable.io

Vulnerability Information

SEVERITY Info
PLUGIN ID 70329
PROTOCOL TCP
LIVE RESULT No

Discovery

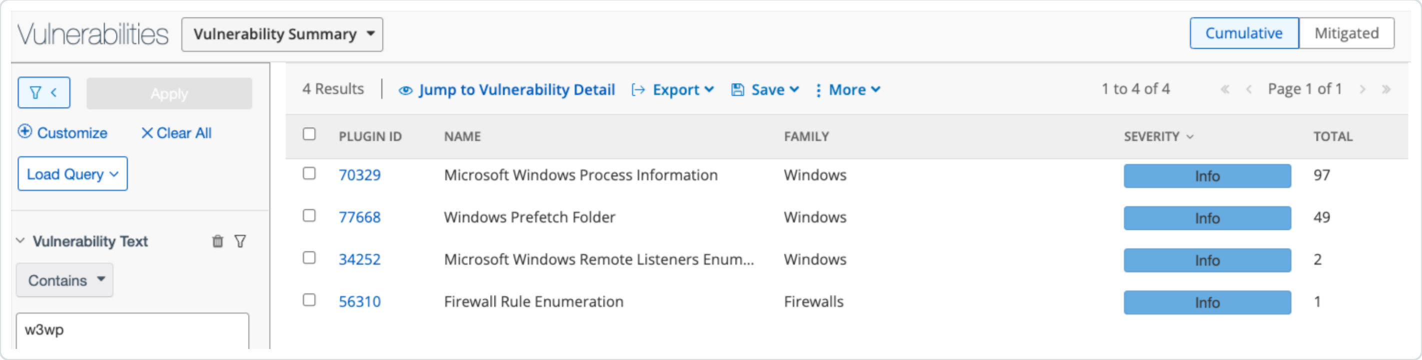
FIRST SEEN 02/09/2022 at 03:03 PM
LAST SEEN 07/31/2023 at 05:24 PM

Description

Report details on the running processes on the machine.

This plugin is informative only and could be used for forensic investigation, malware detection, and to confirm that your system processes conform to your system policies.

The search can be pivoted from Plugin ID to Vulnerability Text. The following image displays all other scan results containing “w3wp” in the plugin output (vulnerability text). This information can now be investigated using the **Vulnerability Detail List** tool or the **Vulnerability List** tool in the drop-down menu above the results.

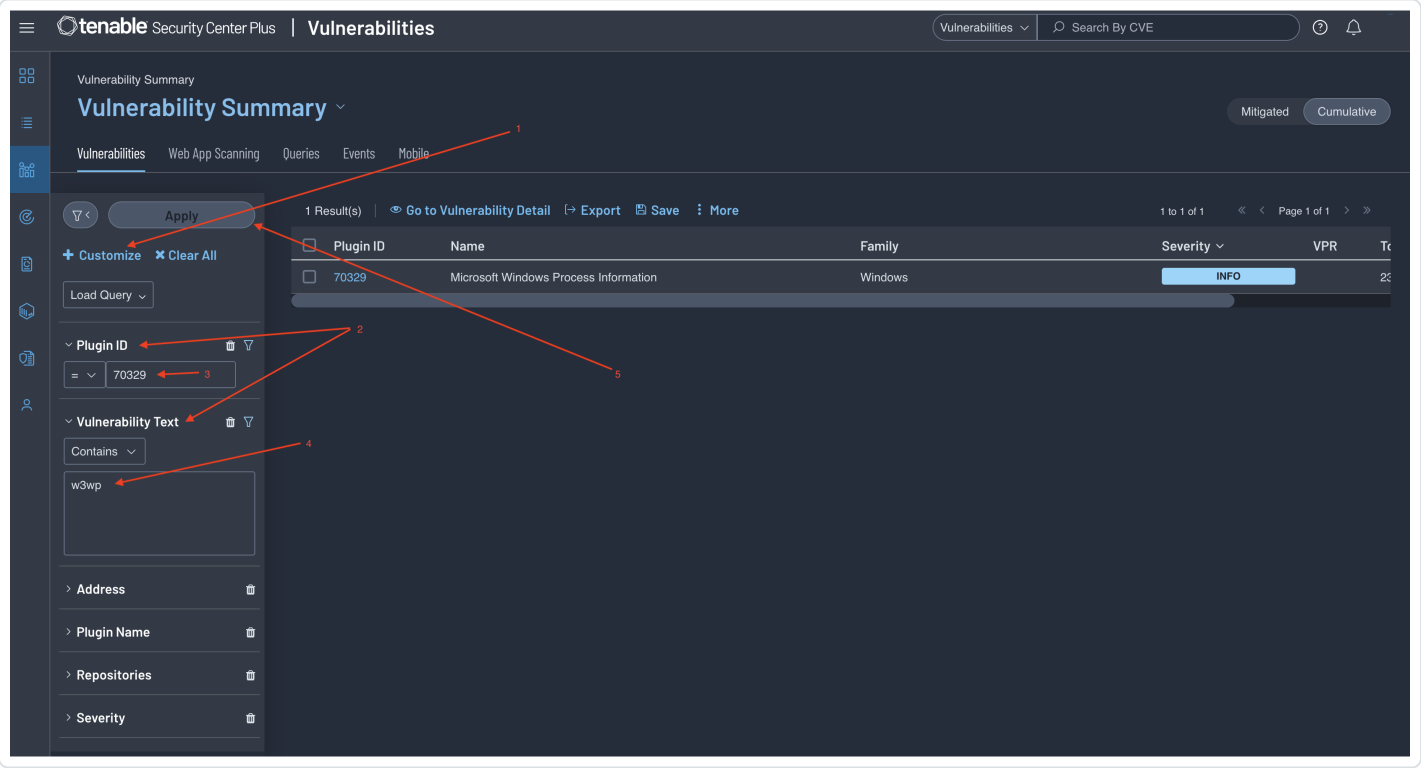


Vulnerability Text: Contains w3wp

4 Results   1 to 4 of 4   Page 1 of 1

PLUGIN ID	NAME	FAMILY	SEVERITY	TOTAL
70329	Microsoft Windows Process Information	Windows	Info	97
77668	Windows Prefetch Folder	Windows	Info	49
34252	Microsoft Windows Remote Listeners Enum...	Windows	Info	2
56310	Firewall Rule Enumeration	Firewalls	Info	1

When using Tenable Security Center the process is similar. However, the starting point is from the Analysis tab, Click on **Customize** (**1**) and select the desired filters for the query, in this example, **Plugin ID** and **Vulnerability Text** (**2**). Deselect any filters, which are not required for the search, by clicking on the check box. Enter the desired Plugin ID for the search (**3**), in this example 70329. Enter the Plugin Output for the search (**4**), in this example "w3wp." Click the Apply button (**5**) to begin the search.



Plugin ID: = 70329

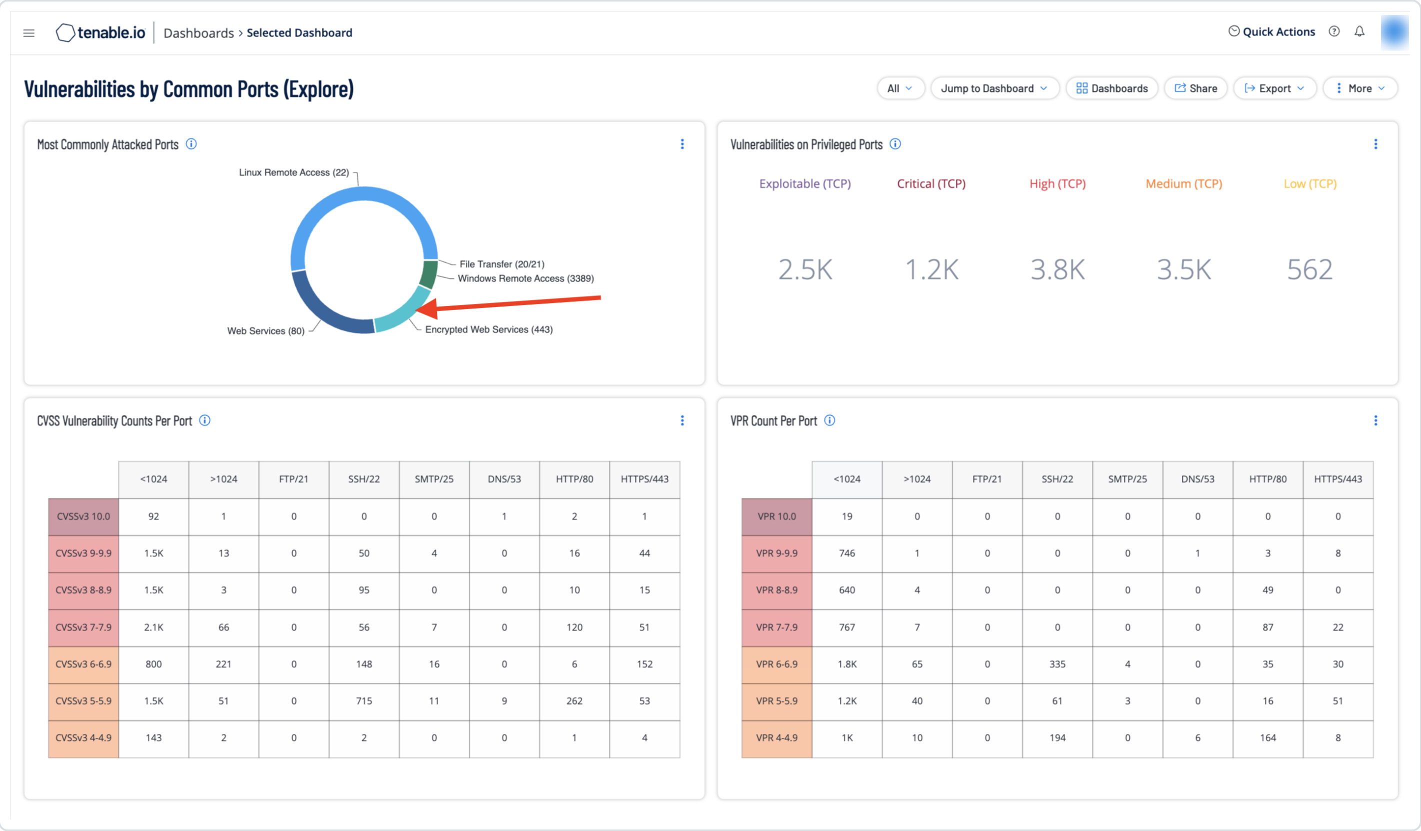
Vulnerability Text: Contains

w3wp

1 Result(s)

Plugin ID	Name	Family	Severity	VPR	Tc
70329	Microsoft Windows Process Information	Windows	INFO		23

Addressing vulnerable services is a key step in reducing network risk. Vulnerable services may allow malicious actors to infiltrate the network, compromise assets, and exfiltrate information. The **Vulnerabilities by Common Ports** (available for both Tenable Vulnerability Management and Tenable Security Center) dashboard presents vulnerability information by common TCP ports and services. Clicking on any cell in the dashboard enables users to drill down into details about the assets on vulnerabilities in each category.



Vulnerabilities by Common Ports (Explore)

Most Commonly Attacked Ports

Vulnerabilities on Privileged Ports

Exploitable (TCP)	Critical (TCP)	High (TCP)	Medium (TCP)	Low (TCP)
2.5K	1.2K	3.8K	3.5K	562

CVSS Vulnerability Counts Per Port

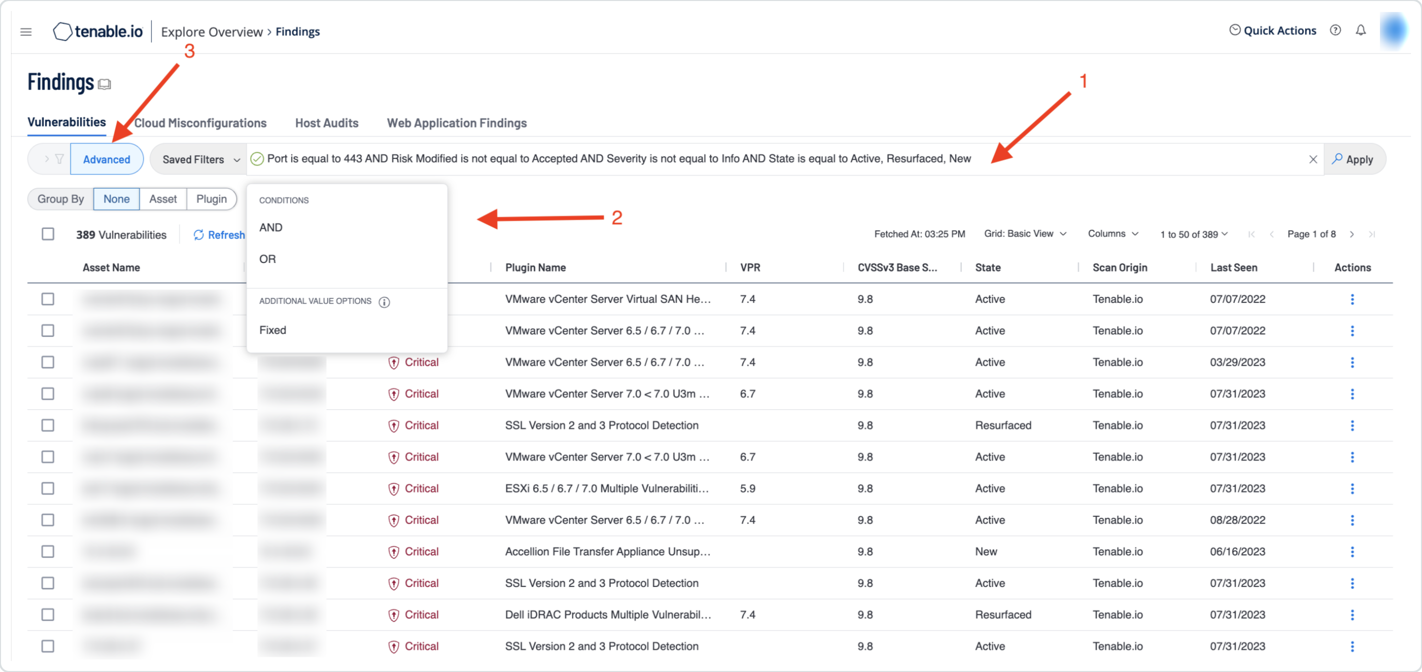
	<1024	>1024	FTP/21	SSH/22	SMTP/25	DNS/53	HTTP/80	HTTPS/443
CVSSv3 10.0	92	1	0	0	0	1	2	1
CVSSv3 9-9.9	1.5K	13	0	50	4	0	16	44
CVSSv3 8-8.9	1.5K	3	0	95	0	0	10	15
CVSSv3 7-7.9	2.1K	66	0	56	7	0	120	51
CVSSv3 6-6.9	800	221	0	148	16	0	6	152
CVSSv3 5-5.9	1.5K	51	0	715	11	9	262	53
CVSSv3 4-4.9	143	2	0	2	0	0	1	4

VPR Count Per Port

	<1024	>1024	FTP/21	SSH/22	SMTP/25	DNS/53	HTTP/80	HTTPS/443
VPR 10.0	19	0	0	0	0	0	0	0
VPR 9-9.9	746	1	0	0	0	1	3	8
VPR 8-8.9	640	4	0	0	0	0	49	0
VPR 7-7.9	767	7	0	0	0	0	87	22
VPR 6-6.9	1.8K	65	0	335	4	0	35	30
VPR 5-5.9	1.2K	40	0	61	3	0	16	51
VPR 4-4.9	1K	10	0	194	0	6	164	8

Drilling Down in Tenable Vulnerability Management

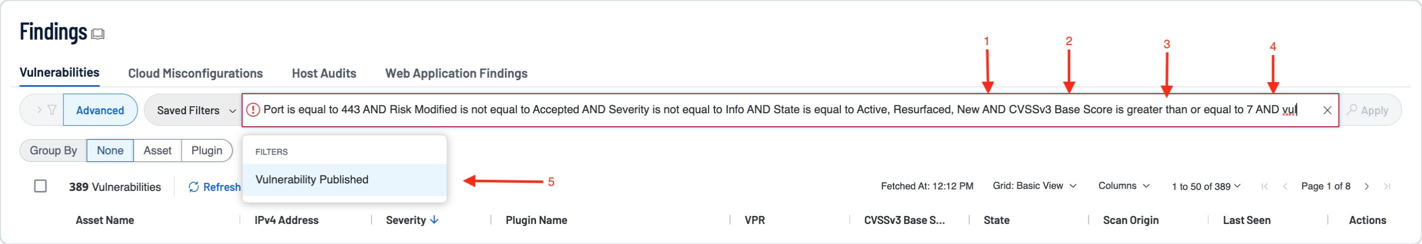
Additional filtering can be performed from either the Conditions field (**1**) or the Advanced (**3**) button. Clicking on the Conditions field opens the Conditions menu (**2**) to refine the filter search.



Port is equal to 443 AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New

Asset Name			Plugin Name	VPR	CVSSv3 Base S...	State	Scan Origin	Last Seen	Actions
[redacted]			VMware vCenter Server Virtual SAN He…	7.4	9.8	Active	Tenable.io	07/07/2022	⋮
[redacted]			VMware vCenter Server 6.5 / 6.7 / 7.0 …	7.4	9.8	Active	Tenable.io	07/07/2022	⋮
[redacted]	[redacted]	Critical	VMware vCenter Server 6.5 / 6.7 / 7.0 …	7.4	9.8	Active	Tenable.io	03/29/2023	⋮
[redacted]	[redacted]	Critical	VMware vCenter Server 7.0 < 7.0 U3m …	6.7	9.8	Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Critical	SSL Version 2 and 3 Protocol Detection		9.8	Resurfaced	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Critical	VMware vCenter Server 7.0 < 7.0 U3m …	6.7	9.8	Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Critical	ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabiliti…	5.9	9.8	Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Critical	VMware vCenter Server 6.5 / 6.7 / 7.0 …	7.4	9.8	Active	Tenable.io	08/28/2022	⋮
[redacted]	[redacted]	Critical	Accellion File Transfer Appliance Unsup…		9.8	New	Tenable.io	06/16/2023	⋮
[redacted]	[redacted]	Critical	SSL Version 2 and 3 Protocol Detection		9.8	Active	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Critical	Dell iDRAC Products Multiple Vulnerabil…	7.4	9.8	Resurfaced	Tenable.io	07/31/2023	⋮
[redacted]	[redacted]	Critical	SSL Version 2 and 3 Protocol Detection		9.8	Active	Tenable.io	07/31/2023	⋮

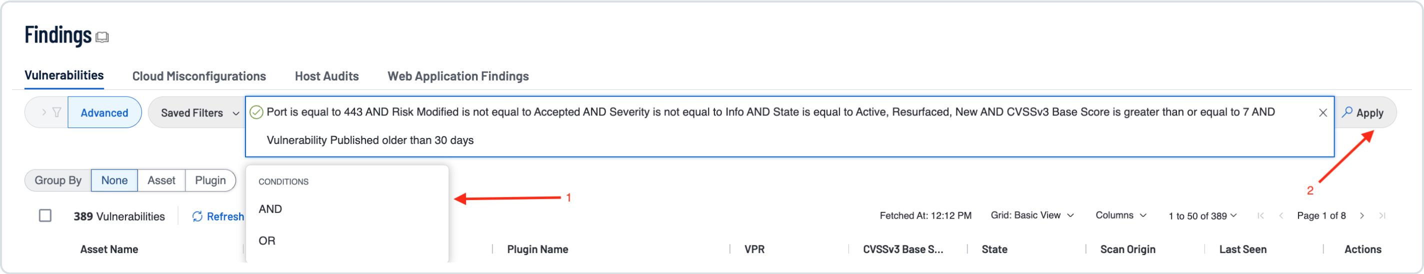
In the example shown in the following image, the **AND** operator was added (**1**) along with **CVSSv3 Base Score** (**2**), then a specification of **greater than or equal to** (**3**), the number **7**, the **AND** operator (**4**), and finally **Vulnerability Published** (**5**).



Port is equal to 443 AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New AND CVSSv3 Base Score is greater than or equal to 7 AND vul

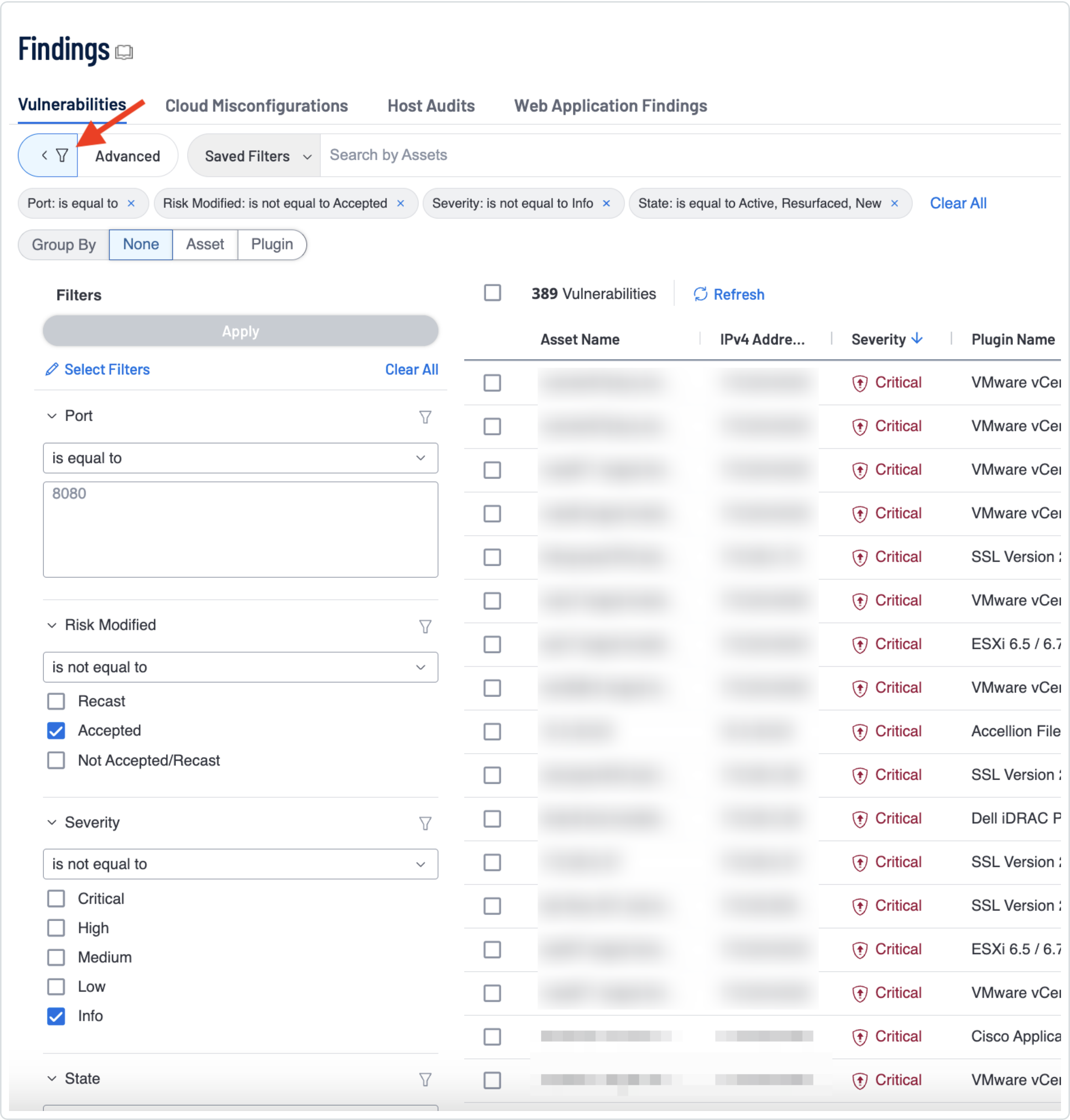
Asset Name	IPv4 Address	Severity	Plugin Name	VPR	CVSSv3 Base S...	State	Scan Origin	Last Seen	Actions

Additional conditions can be added (**1**) or the filter can be applied by clicking on the **Apply** (**2**) button, as shown in the following image:



Port is equal to 443 AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New AND CVSSv3 Base Score is greater than or equal to 7 AND Vulnerability Published older than 30 days

Another method to filter queries is to click on the filter button next to the Advanced button, which displays a user interface, as shown in the following image:



Findings

Port: is equal to × | Risk Modified: is not equal to Accepted × | Severity: is not equal to Info × | State: is equal to Active, Resurfaced, New × | Clear All

Filters

Port

is equal to

8080

Risk Modified

is not equal to

- ☐ Recast
- ☑ Accepted
- ☐ Not Accepted/Recast

Severity

is not equal to

- ☐ Critical
- ☐ High
- ☐ Medium
- ☐ Low
- ☑ Info

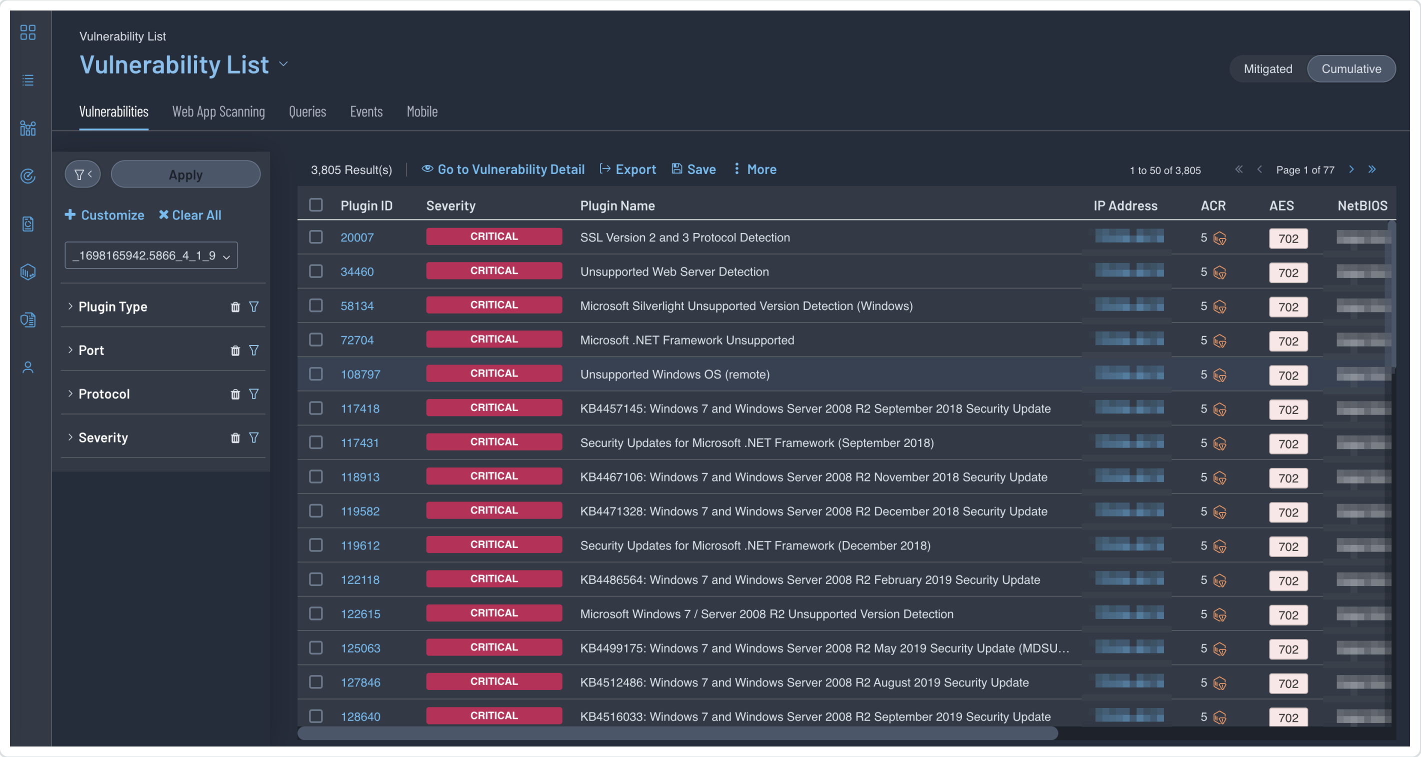
State

389 Vulnerabilities

Asset Name	IPv4 Addre...	Severity ↓	Plugin Name
[redacted]	[redacted]	Critical	VMware vCe
[redacted]	[redacted]	Critical	VMware vCe
[redacted]	[redacted]	Critical	VMware vCe
[redacted]	[redacted]	Critical	VMware vCe
[redacted]	[redacted]	Critical	SSL Version
[redacted]	[redacted]	Critical	VMware vCe
[redacted]	[redacted]	Critical	ESXi 6.5 / 6.7
[redacted]	[redacted]	Critical	VMware vCe
[redacted]	[redacted]	Critical	Accellion File
[redacted]	[redacted]	Critical	SSL Version
[redacted]	[redacted]	Critical	Dell iDRAC P
[redacted]	[redacted]	Critical	SSL Version
[redacted]	[redacted]	Critical	SSL Version
[redacted]	[redacted]	Critical	ESXi 6.5 / 6.7
[redacted]	[redacted]	Critical	VMware vCe
[redacted]	[redacted]	Critical	Cisco Applica
[redacted]	[redacted]	Critical	VMware vCe

Drilling Down in Tenable Security Center

Additional filtering can be performed to reduce the number of returned vulnerabilities by clicking into a cell or if you are viewing a table clicking on **View Data >** will take you to the Vulnerability Analysis page.

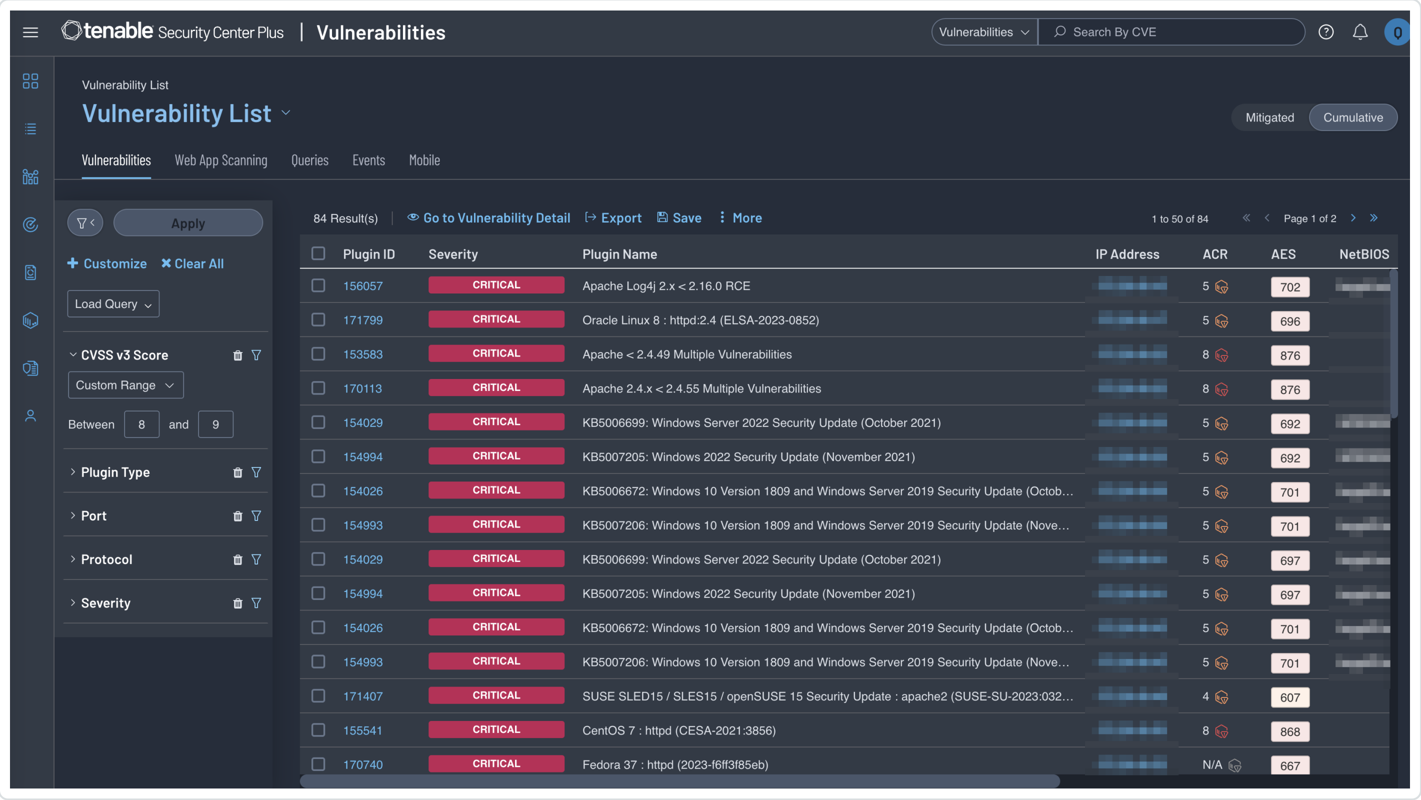


3,805 Result(s)

1 to 50 of 3,805 Page 1 of 77

□	Plugin ID	Severity	Plugin Name	IP Address	ACR	AES	NetBIOS
□	20007	CRITICAL	SSL Version 2 and 3 Protocol Detection	[redacted]	5	702	[redacted]
□	34460	CRITICAL	Unsupported Web Server Detection	[redacted]	5	702	[redacted]
□	58134	CRITICAL	Microsoft Silverlight Unsupported Version Detection (Windows)	[redacted]	5	702	[redacted]
□	72704	CRITICAL	Microsoft .NET Framework Unsupported	[redacted]	5	702	[redacted]
□	108797	CRITICAL	Unsupported Windows OS (remote)	[redacted]	5	702	[redacted]
□	117418	CRITICAL	KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update	[redacted]	5	702	[redacted]
□	117431	CRITICAL	Security Updates for Microsoft .NET Framework (September 2018)	[redacted]	5	702	[redacted]
□	118913	CRITICAL	KB4467106: Windows 7 and Windows Server 2008 R2 November 2018 Security Update	[redacted]	5	702	[redacted]
□	119582	CRITICAL	KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update	[redacted]	5	702	[redacted]
□	119612	CRITICAL	Security Updates for Microsoft .NET Framework (December 2018)	[redacted]	5	702	[redacted]
□	122118	CRITICAL	KB4486564: Windows 7 and Windows Server 2008 R2 February 2019 Security Update	[redacted]	5	702	[redacted]
□	122615	CRITICAL	Microsoft Windows 7 / Server 2008 R2 Unsupported Version Detection	[redacted]	5	702	[redacted]
□	125063	CRITICAL	KB4499175: Windows 7 and Windows Server 2008 R2 May 2019 Security Update (MDSU…	[redacted]	5	702	[redacted]
□	127846	CRITICAL	KB4512486: Windows 7 and Windows Server 2008 R2 August 2019 Security Update	[redacted]	5	702	[redacted]
□	128640	CRITICAL	KB4516033: Windows 7 and Windows Server 2008 R2 September 2019 Security Update	[redacted]	5	702	[redacted]

In the following example, a filter for **CVSS v3 Score (1)** along with a custom range specification of **between 9**, and **7 (2)**.



CVSS v3 Score: Custom Range, Between 8 and 9

84 Result(s) | 1 to 50 of 84 | Page 1 of 2

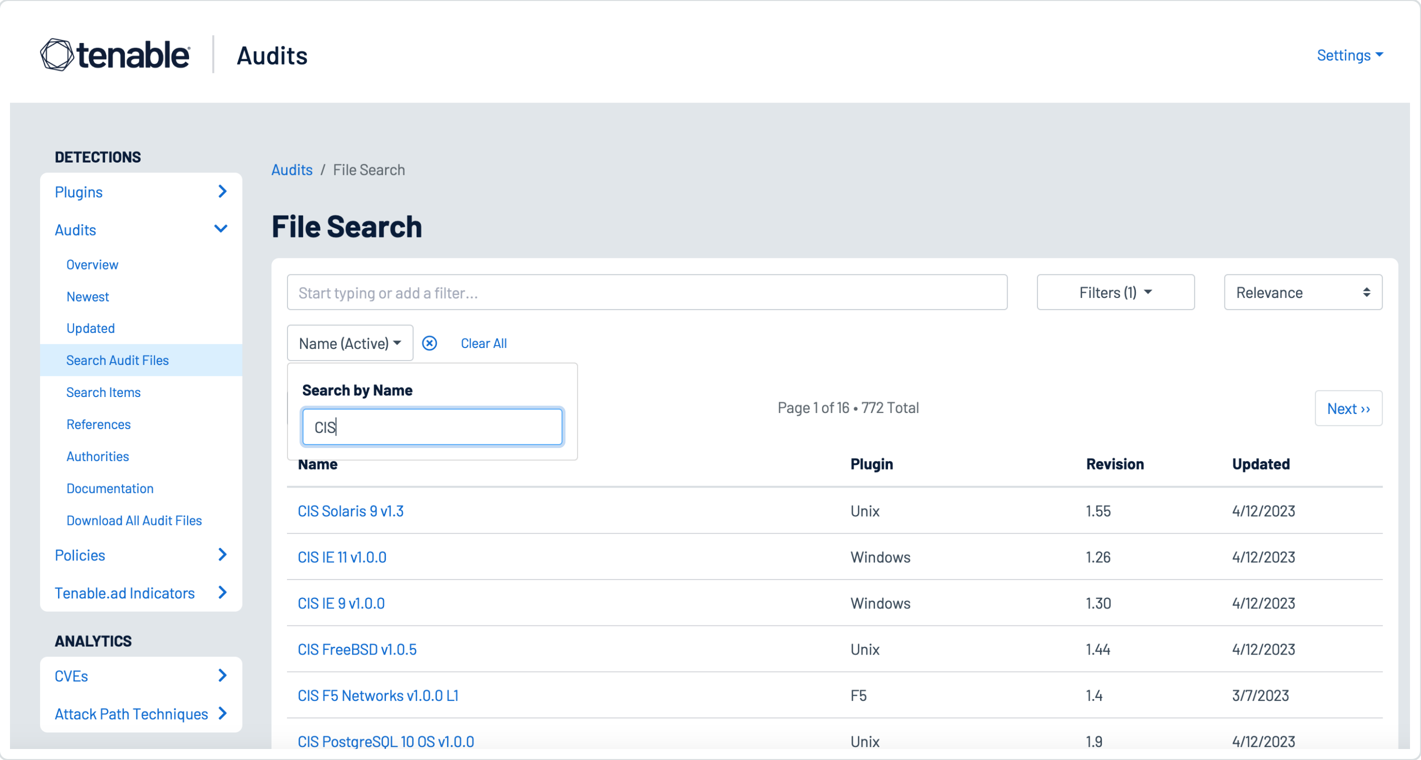
Plugin ID	Severity	Plugin Name	IP Address	ACR	AES	NetBIOS
156057	CRITICAL	Apache Log4j 2.x < 2.16.0 RCE	[redacted]	5	702	[redacted]
171799	CRITICAL	Oracle Linux 8 : httpd:2.4 (ELSA-2023-0852)	[redacted]	5	696	
153583	CRITICAL	Apache < 2.4.49 Multiple Vulnerabilities	[redacted]	8	876	
170113	CRITICAL	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	[redacted]	8	876	
154029	CRITICAL	KB5006699: Windows Server 2022 Security Update (October 2021)	[redacted]	5	692	[redacted]
154994	CRITICAL	KB5007205: Windows 2022 Security Update (November 2021)	[redacted]	5	692	[redacted]
154026	CRITICAL	KB5006672: Windows 10 Version 1809 and Windows Server 2019 Security Update (Octob…	[redacted]	5	701	[redacted]
154993	CRITICAL	KB5007206: Windows 10 Version 1809 and Windows Server 2019 Security Update (Nove…	[redacted]	5	701	[redacted]
154029	CRITICAL	KB5006699: Windows Server 2022 Security Update (October 2021)	[redacted]	5	697	[redacted]
154994	CRITICAL	KB5007205: Windows 2022 Security Update (November 2021)	[redacted]	5	697	[redacted]
154026	CRITICAL	KB5006672: Windows 10 Version 1809 and Windows Server 2019 Security Update (Octob…	[redacted]	5	701	[redacted]
154993	CRITICAL	KB5007206: Windows 10 Version 1809 and Windows Server 2019 Security Update (Nove…	[redacted]	5	701	[redacted]
171407	CRITICAL	SUSE SLED15 / SLES15 / openSUSE 15 Security Update : apache2 (SUSE-SU-2023:032…	[redacted]	4	607	
155541	CRITICAL	CentOS 7 : httpd (CESA-2021:3856)	[redacted]	8	868	
170740	CRITICAL	Fedora 37 : httpd (2023-f6ff3f85eb)	[redacted]	N/A	667	

Application Server Hardening

Application server hardening is the process of securing and fortifying an application server to reduce the device's exposure to potential threats and vulnerabilities. Even if an application is written following the best application security practices, the application can still be vulnerable if the server the application is running on is not secure. Multiple layers of defense must be addressed, including those not just limited to the application itself, but also to the host and operating system. Hardening involves implementing various security measures and established standards to enhance the device's resilience against attacks and unauthorized access. The primary goal is to reduce the attack surface and ensure the server and the applications remain available.

Application and server hardening comprises many of the aspects discussed in this guide, such as: configuring minimal privileges, disabling unnecessary services, keeping software up-to-date, secure communications, protection against common web application vulnerabilities, and periodic vulnerability scans. Application hardening is an ongoing process. Regularly assess the device's security posture, stay informed about the latest threats and vulnerabilities, and update hardening measures accordingly. Compliance scanning is a great place to start the process.

Compliance scanning is accomplished by conducting compliance checks using specific audit files and privileged credentials added to the scan policy. Use the [Tenable Audit Search]() page with the Name filter to search for system hardening audits, such as the [CIS Benchmarks](), as shown in the following image for Tenable Vulnerability Management:



File Search

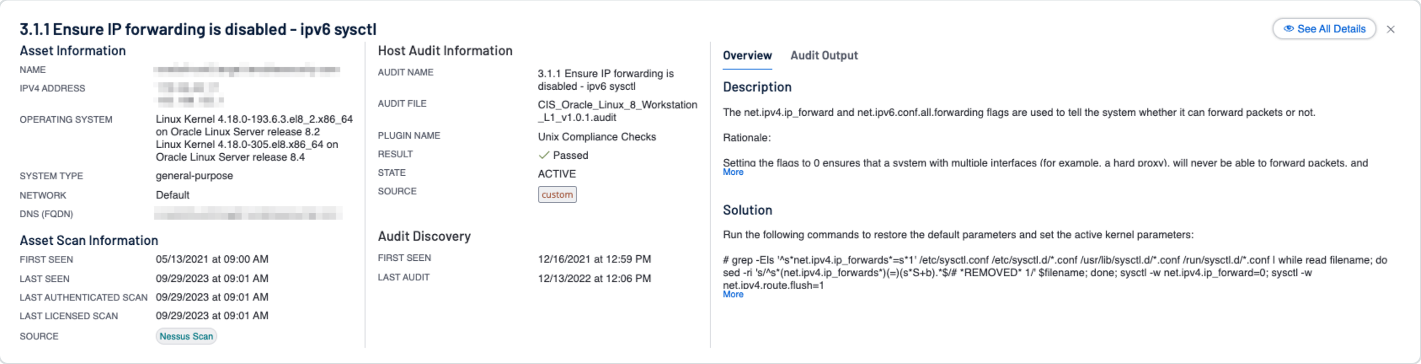
Name (Active)

Search by Name: CIS

Page 1 of 16 • 772 Total

Name	Plugin	Revision	Updated
CIS Solaris 9 v1.3	Unix	1.55	4/12/2023
CIS IE 11 v1.0.0	Windows	1.26	4/12/2023
CIS IE 9 v1.0.0	Windows	1.30	4/12/2023
CIS FreeBSD v1.0.5	Unix	1.44	4/12/2023
CIS F5 Networks v1.0.0 L1	F5	1.4	3/7/2023
CIS PostgreSQL 10 OS v1.0.0	Unix	1.9	4/12/2023

Host audit findings details can be found on the **Findings** page within Tenable Vulnerability Management. Click on a host audit finding to preview the details in the panel.



3.1.1 Ensure IP forwarding is disabled - ipv6 sysctl

Asset Information

NAME	[redacted]
IPV4 ADDRESS	[redacted]
OPERATING SYSTEM	Linux Kernel 4.18.0-193.6.3.el8_2.x86_64 on Oracle Linux Server release 8.2 Linux Kernel 4.18.0-305.el8.x86_64 on Oracle Linux Server release 8.4
SYSTEM TYPE	general-purpose
NETWORK	Default
DNS (FQDN)	[redacted]

Asset Scan Information

FIRST SEEN	05/13/2021 at 09:00 AM
LAST SEEN	09/29/2023 at 09:01 AM
LAST AUTHENTICATED SCAN	09/29/2023 at 09:01 AM
LAST LICENSED SCAN	09/29/2023 at 09:01 AM
SOURCE	Nessus Scan

Host Audit Information

AUDIT NAME	3.1.1 Ensure IP forwarding is disabled - ipv6 sysctl
AUDIT FILE	CIS_Oracle_Linux_8_Workstation_L1_v1.0.1.audit
PLUGIN NAME	Unix Compliance Checks
RESULT	✓ Passed
STATE	ACTIVE
SOURCE	custom

Audit Discovery

FIRST SEEN	12/16/2021 at 12:59 PM
LAST AUDIT	12/13/2022 at 12:06 PM

Description

The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not.

Rationale:

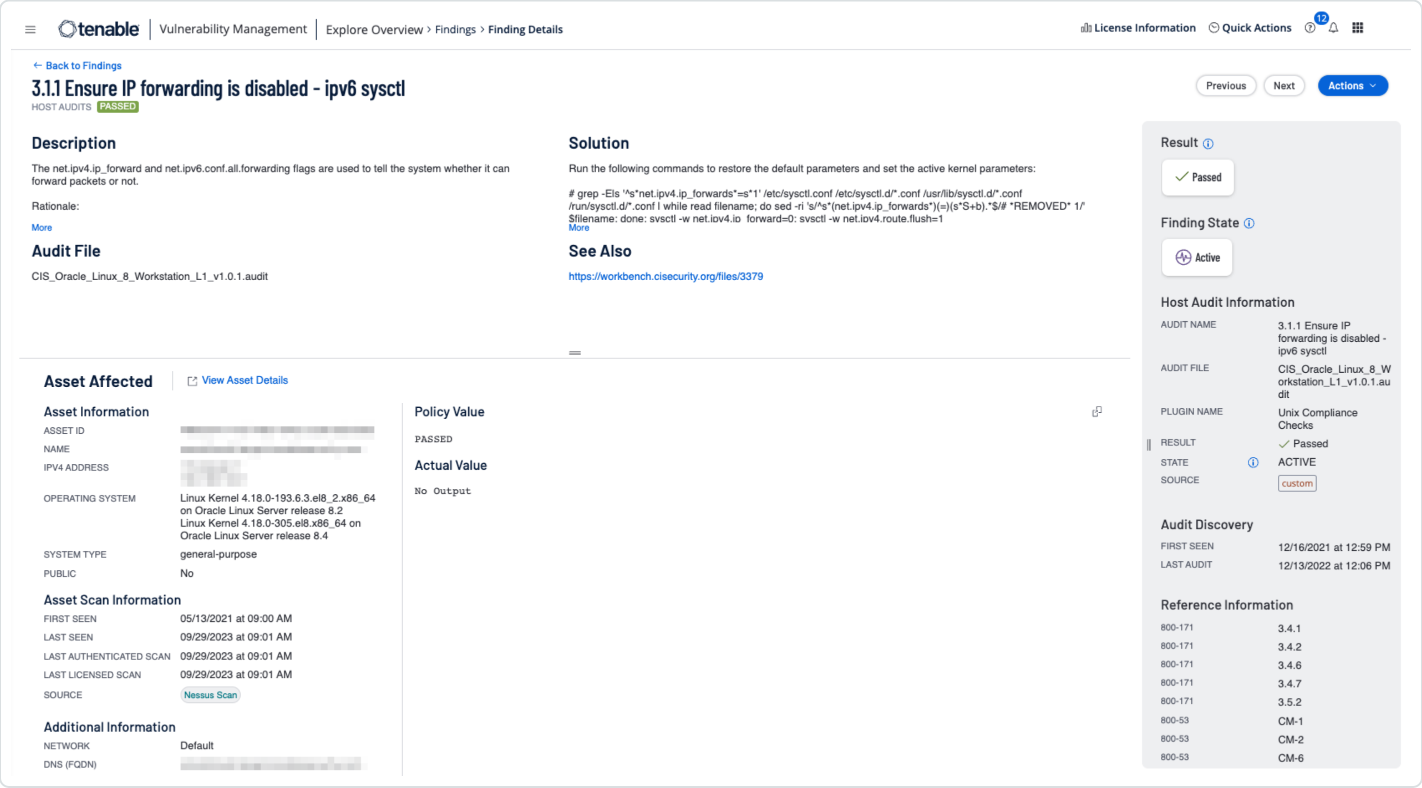
Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and

Solution

Run the following commands to restore the default parameters and set the active kernel parameters:

```
# grep -Els '^s*net.ipv4.ip_forwards*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf /run/sysctl.d/*.conf | while read filename; do
sed -ri 's/^s*(net.ipv4.ip_forwards*)(=)(s*S+b).*$/# *REMOVED* 1/' $filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w
net.ipv4.route.flush=1
```

Select **See All Details** to open the details page. Details also contain the name of the audit file used.



3.1.1 Ensure IP forwarding is disabled - ipv6 sysctl

HOST AUDITS PASSED

Description

The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not.

Rationale:

More

Solution

Run the following commands to restore the default parameters and set the active kernel parameters:

```
# grep -Els '^s*net.ipv4.ip_forwards*=s*1' /etc/sysctl.conf /etc/sysctl.d/*.conf /usr/lib/sysctl.d/*.conf
/run/sysctl.d/*.conf I while read filename; do sed -ri 's/^s*(net.ipv4.ip_forwards*)(=)(s*S+b).*$/# *REMOVED* 1/'
$filename; done; sysctl -w net.ipv4.ip_forward=0; sysctl -w net.ipv4.route.flush=1
```

More

Audit File

CIS_Oracle_Linux_8_Workstation_L1_v1.0.1.audit

See Also

https://workbench.cisecurity.org/files/3379

Asset Affected View Asset Details

Asset Information

ASSET ID	[redacted]
NAME	[redacted]
IPV4 ADDRESS	[redacted]
OPERATING SYSTEM	Linux Kernel 4.18.0-193.6.3.el8_2.x86_64 on Oracle Linux Server release 8.2 Linux Kernel 4.18.0-305.el8.x86_64 on Oracle Linux Server release 8.4
SYSTEM TYPE	general-purpose
PUBLIC	No

Asset Scan Information

FIRST SEEN	05/13/2021 at 09:00 AM
LAST SEEN	09/29/2023 at 09:01 AM
LAST AUTHENTICATED SCAN	09/29/2023 at 09:01 AM
LAST LICENSED SCAN	09/29/2023 at 09:01 AM
SOURCE	Nessus Scan

Additional Information

NETWORK	Default
DNS (FQDN)	[redacted]

Policy Value

```
PASSED
```

Actual Value

```
No Output
```

Result

✓ Passed

Finding State

Active

Host Audit Information

AUDIT NAME	3.1.1 Ensure IP forwarding is disabled - ipv6 sysctl
AUDIT FILE	CIS_Oracle_Linux_8_Workstation_L1_v1.0.1.audit
PLUGIN NAME	Unix Compliance Checks
RESULT	✓ Passed
STATE	ACTIVE
SOURCE	custom

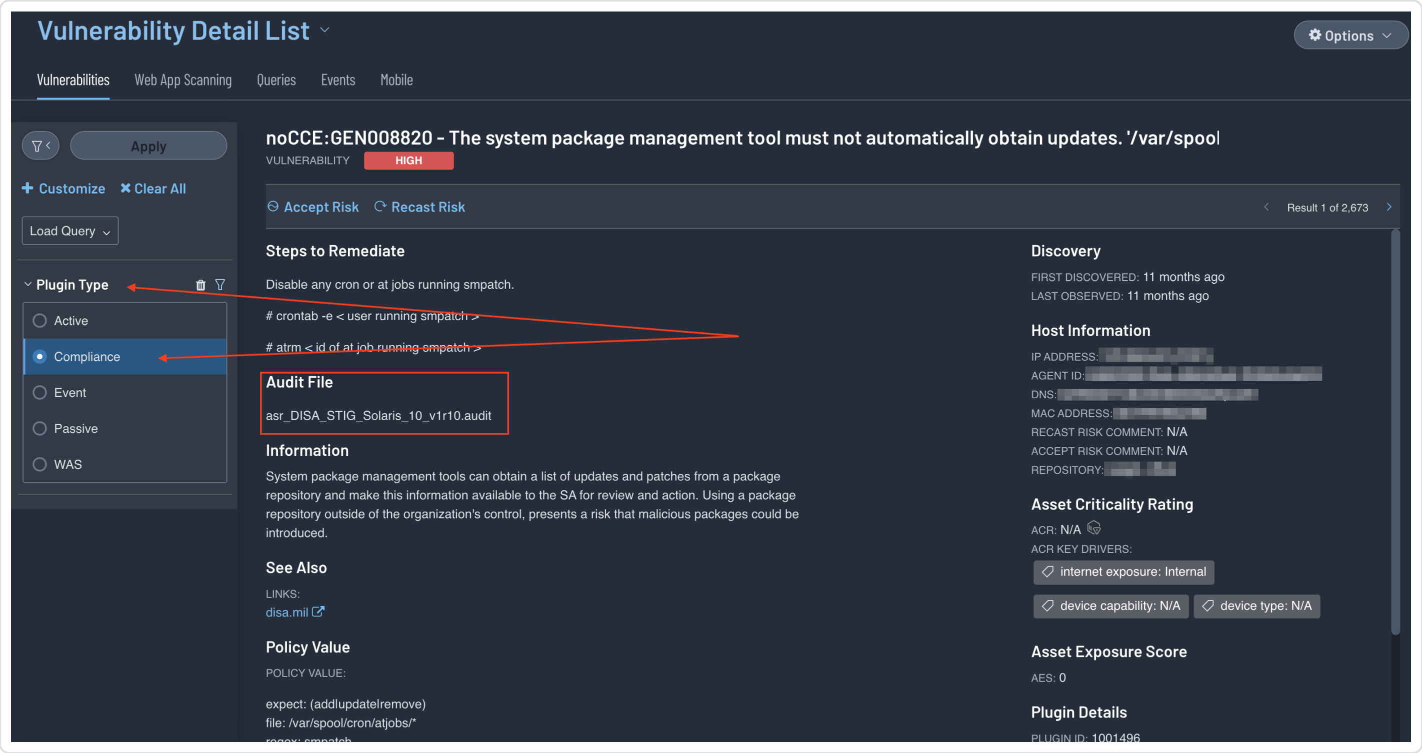
Audit Discovery

FIRST SEEN	12/16/2021 at 12:59 PM
LAST AUDIT	12/13/2022 at 12:06 PM

Reference Information

800-171	3.4.1
800-171	3.4.2
800-171	3.4.6
800-171	3.4.7
800-171	3.5.2
800-53	CM-1
800-53	CM-2
800-53	CM-6

For Tenable Security Center, compliance results can be displayed by using the Plugin Type filter, and selecting the compliance radio button as shown below. Viewing the detailed information is similar to Tenable VM, and the audit file used will also be displayed in the detailed results as shown in the following image:



noCCE:GEN008820 - The system package management tool must not automatically obtain updates. '/var/spool

VULNERABILITY HIGH

Steps to Remediate

Disable any cron or at jobs running smpatch.

```
# crontab -e < user running smpatch >
# atrm < id of at job running smpatch >
```

Audit File

asr_DISA_STIG_Solaris_10_v1r10.audit

Information

System package management tools can obtain a list of updates and patches from a package repository and make this information available to the SA for review and action. Using a package repository outside of the organization's control, presents a risk that malicious packages could be introduced.

See Also

LINKS:
disa.mil

Policy Value

POLICY VALUE:

```
expect: (add|update|remove)
file: /var/spool/cron/atjobs/*
regex: smpatch
```

Discovery

FIRST DISCOVERED: 11 months ago
LAST OBSERVED: 11 months ago

Host Information

IP ADDRESS: [redacted]
AGENT ID: [redacted]
DNS: [redacted]
MAC ADDRESS: [redacted]
RECAST RISK COMMENT: N/A
ACCEPT RISK COMMENT: N/A
REPOSITORY: [redacted]

Asset Criticality Rating

ACR: N/A
ACR KEY DRIVERS:
internet exposure: Internal
device capability: N/A
device type: N/A

Asset Exposure Score

AES: 0

Plugin Details

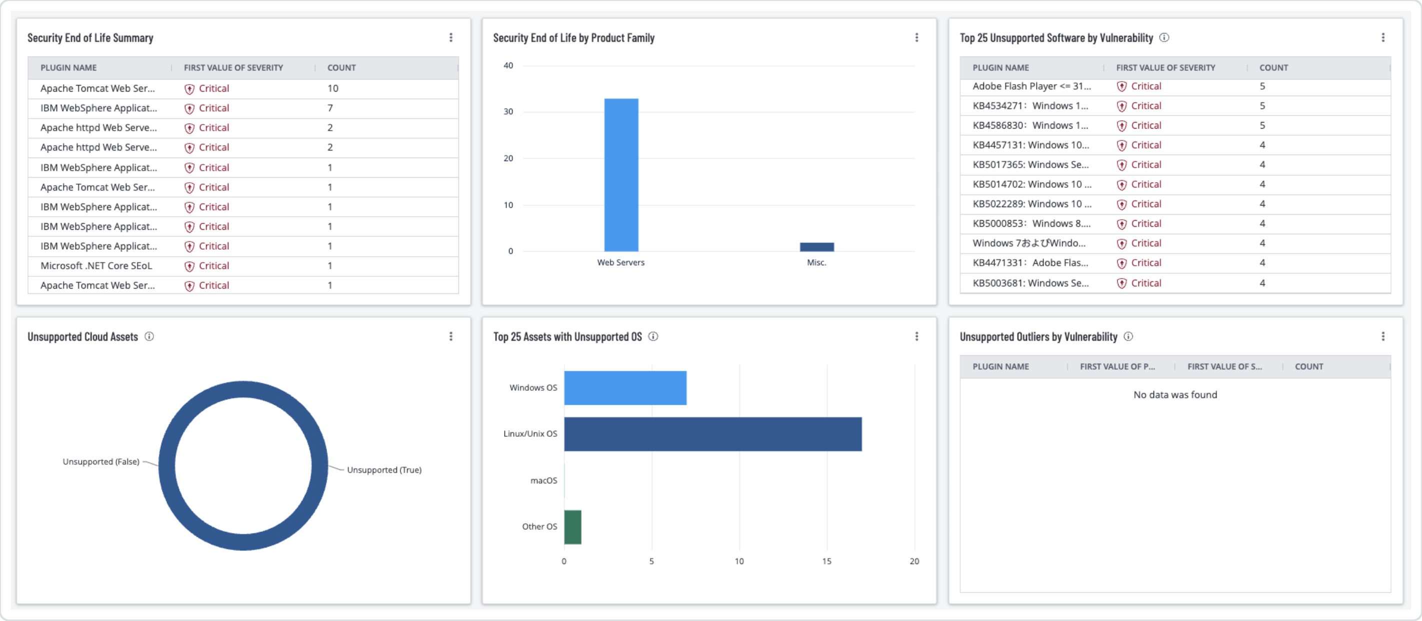
PLUGIN ID: 1001496

Unsupported Software

Identifying assets running End of Life (EOL) applications is an important part of assessing and minimizing organizational risk since patches, updates, and security fixes are no longer available. Many standards state organizations must ensure that only software applications or operating systems that are 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.

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. Tenable 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 identity areas for risk mitigation.

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



Security End of Life Summary

PLUGIN NAME	FIRST VALUE OF SEVERITY	COUNT
Apache Tomcat Web Ser...	Critical	10
IBM WebSphere Applicat...	Critical	7
Apache httpd Web Serve...	Critical	2
Apache httpd Web Serve...	Critical	2
IBM WebSphere Applicat...	Critical	1
Apache Tomcat Web Ser...	Critical	1
IBM WebSphere Applicat...	Critical	1
IBM WebSphere Applicat...	Critical	1
IBM WebSphere Applicat...	Critical	1
Microsoft .NET Core SEoL	Critical	1
Apache Tomcat Web Ser...	Critical	1

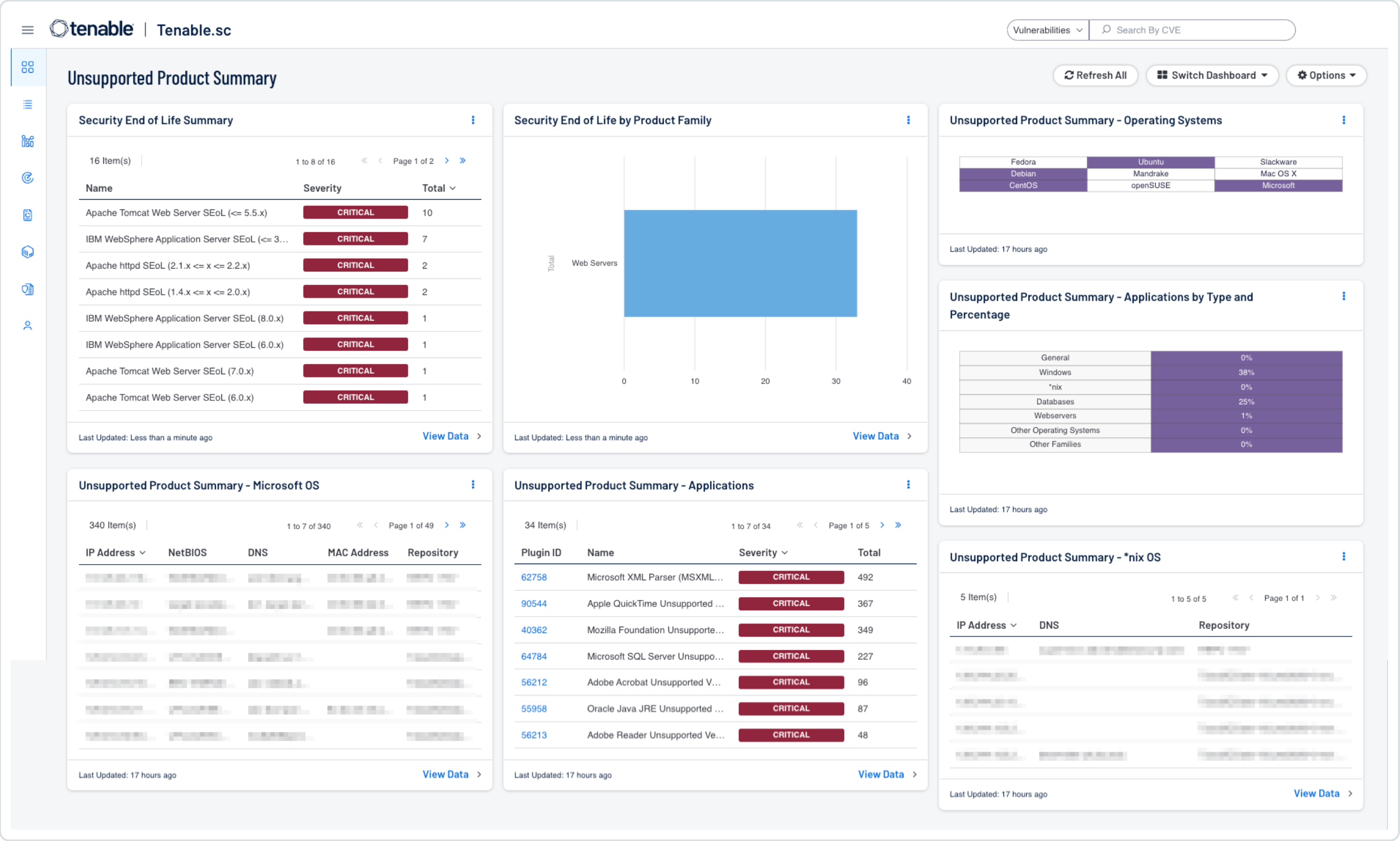
Top 25 Unsupported Software by Vulnerability

PLUGIN NAME	FIRST VALUE OF SEVERITY	COUNT
Adobe Flash Player <= 31...	Critical	5
KB4534271： Windows 1...	Critical	5
KB4586830： Windows 1...	Critical	5
KB4457131: Windows 10...	Critical	4
KB5017365: Windows Se...	Critical	4
KB5014702: Windows 10 ...	Critical	4
KB5022289: Windows 10 ...	Critical	4
KB5000853： Windows 8....	Critical	4
Windows 7およびWindo...	Critical	4
KB4471331： Adobe Flas...	Critical	4
KB5003681: Windows Se...	Critical	4

Unsupported Outliers by Vulnerability

PLUGIN NAME	FIRST VALUE OF P...	FIRST VALUE OF S...	COUNT
No data was found			

For Tenable Security Center customers, the Unsupported Product Summary displays details of unsupported (end-of-life) products found in the environment.



Unsupported Product Summary

Security End of Life Summary

16 Item(s) | 1 to 8 of 16 | Page 1 of 2

Name	Severity	Total
Apache Tomcat Web Server SEoL (<= 5.5.x)	CRITICAL	10
IBM WebSphere Application Server SEoL (<= 3…	CRITICAL	7
Apache httpd SEoL (2.1.x <= x <= 2.2.x)	CRITICAL	2
Apache httpd SEoL (1.4.x <= x <= 2.0.x)	CRITICAL	2
IBM WebSphere Application Server SEoL (8.0.x)	CRITICAL	1
IBM WebSphere Application Server SEoL (6.0.x)	CRITICAL	1
Apache Tomcat Web Server SEoL (7.0.x)	CRITICAL	1
Apache Tomcat Web Server SEoL (6.0.x)	CRITICAL	1

Last Updated: Less than a minute ago   View Data

Security End of Life by Product Family

Last Updated: Less than a minute ago   View Data

Unsupported Product Summary - Operating Systems

Fedora	Ubuntu	Slackware
Debian	Mandrake	Mac OS X
CentOS	openSUSE	Microsoft

Last Updated: 17 hours ago

Unsupported Product Summary - Applications by Type and Percentage

General	0%
Windows	38%
*nix	0%
Databases	25%
Webservers	1%
Other Operating Systems	0%
Other Families	0%

Last Updated: 17 hours ago

Unsupported Product Summary - Microsoft OS

340 Item(s) | 1 to 7 of 340 | Page 1 of 49

IP Address	NetBIOS	DNS	MAC Address	Repository
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]		[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]		[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]		[redacted]

Last Updated: 17 hours ago   View Data

Unsupported Product Summary - Applications

34 Item(s) | 1 to 7 of 34 | Page 1 of 5

Plugin ID	Name	Severity	Total
62758	Microsoft XML Parser (MSXML…	CRITICAL	492
90544	Apple QuickTime Unsupported …	CRITICAL	367
40362	Mozilla Foundation Unsupporte…	CRITICAL	349
64784	Microsoft SQL Server Unsuppo…	CRITICAL	227
56212	Adobe Acrobat Unsupported V…	CRITICAL	96
55958	Oracle Java JRE Unsupported …	CRITICAL	87
56213	Adobe Reader Unsupported Ve…	CRITICAL	48

Last Updated: 17 hours ago   View Data

Unsupported Product Summary - *nix OS

5 Item(s) | 1 to 5 of 5 | Page 1 of 1

IP Address	DNS	Repository
[redacted]	[redacted]	[redacted]
[redacted]		[redacted]
[redacted]		[redacted]
[redacted]		[redacted]
[redacted]	[redacted]	[redacted]

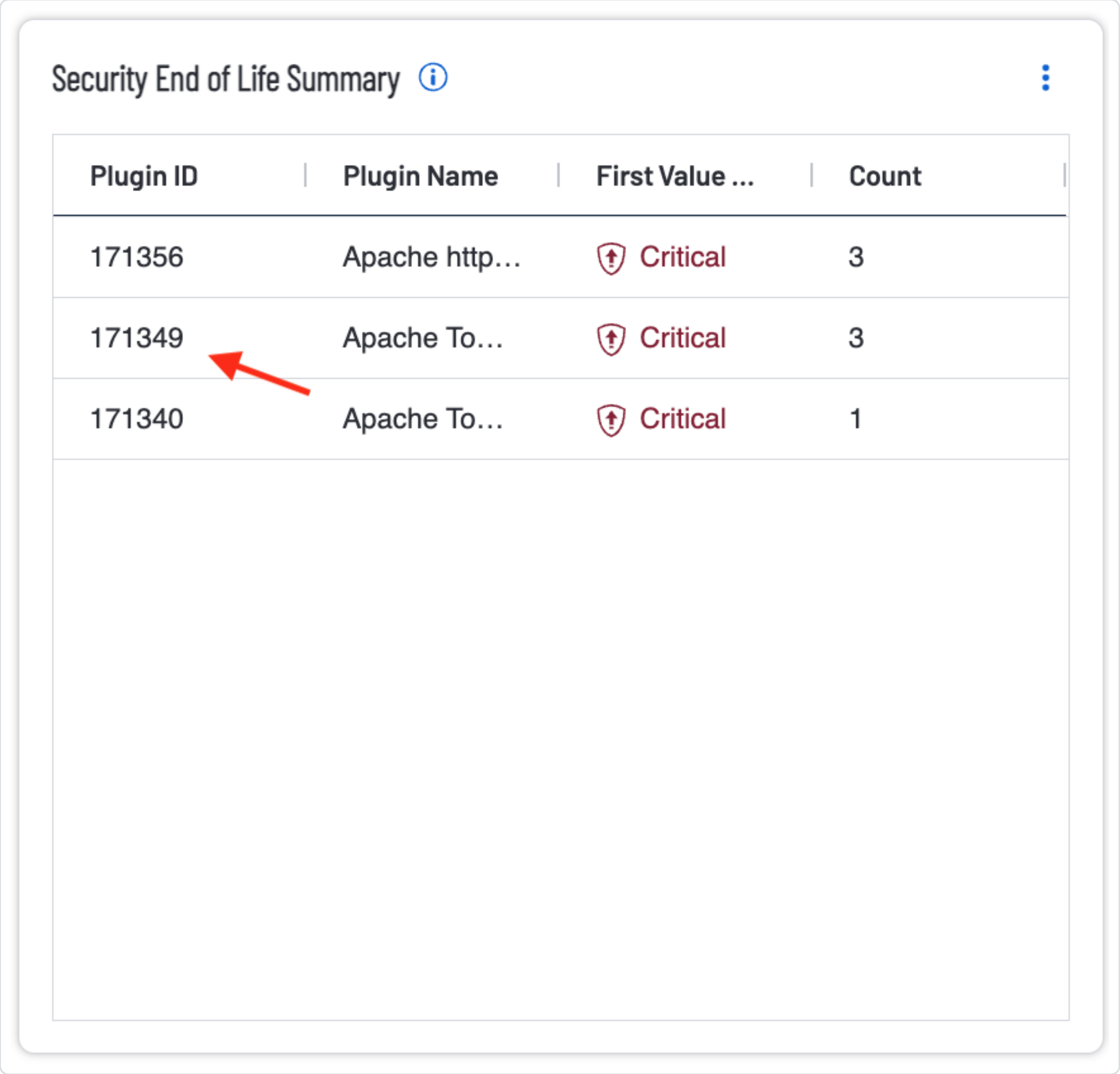
Last Updated: 17 hours ago   View Data

Security End of Life

The **Security End of Life** widget (Tenable Vulnerability Management) and the **Security End of Life Summary** component (Tenable Security Center) displays information about products that have entered the Security End of Life state of the Security Maintenance Lifecycle. This component utilizes a filter containing the string 'SEoL' (Security End of Life) contained in the plugin name to identify these specific vulnerabilities. These plugins can be identified by looking at the plugin name which will contain the string 'SEoL', such as 'Apache httpd SEoL (2.1.x <= x <= 2.2.x)'. The new plugins provide a structured output and consistent updates to the content

Drill Down for Tenable Vulnerability Management

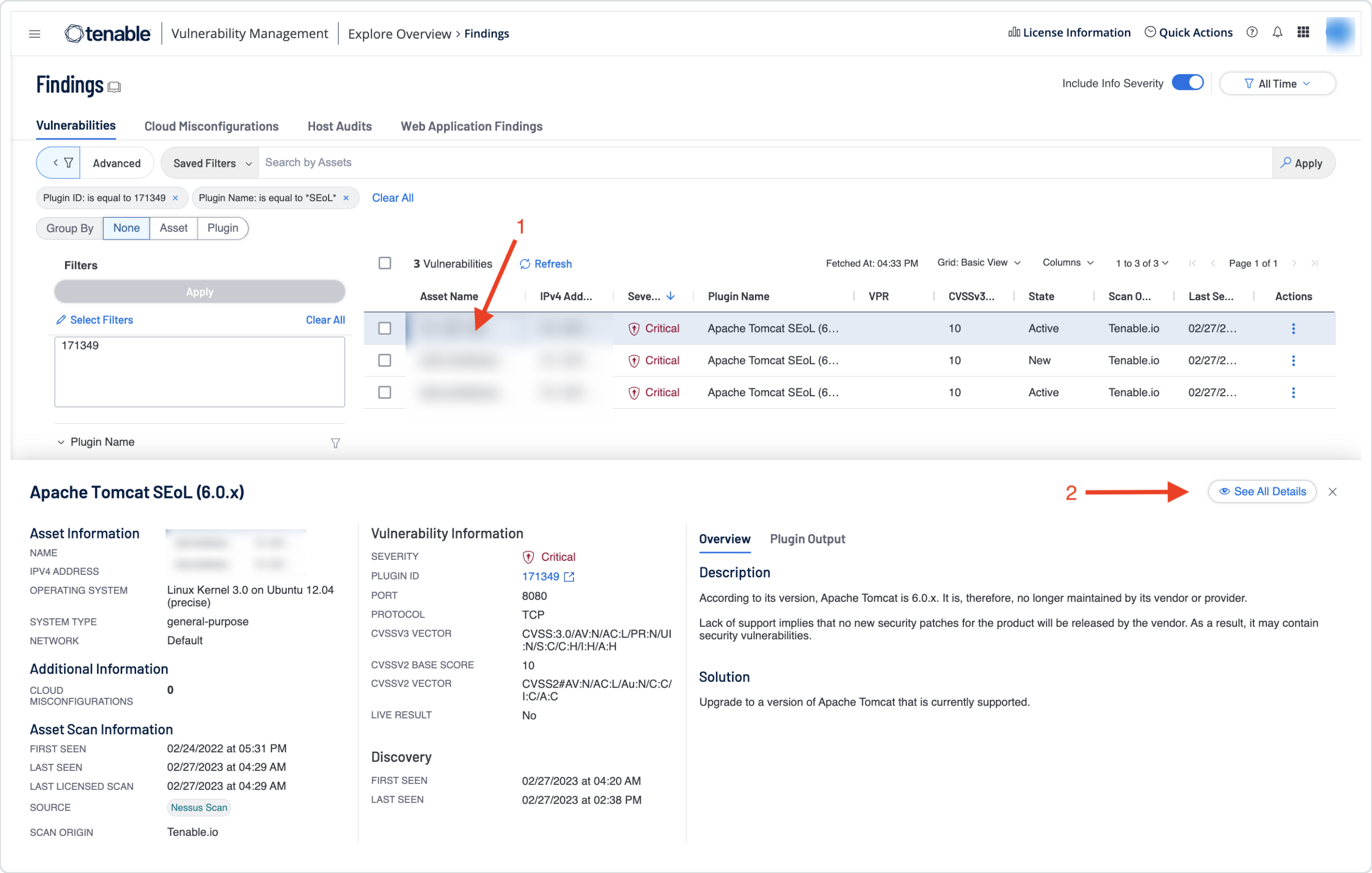
Drilling down into the data presents a vulnerability summary where additional details on each identified SEoL finding can be viewed. Click on a cell to drill into the Findings page for more details and to perform refined searches.



Security End of Life Summary

Plugin ID	Plugin Name	First Value ...	Count
171356	Apache http...	Critical	3
171349	Apache To...	Critical	3
171340	Apache To...	Critical	1

For more details, click on an asset (**1**) and select **See All Details** (**2**).



Findings

Include Info Severity · All Time

Vulnerabilities · Cloud Misconfigurations · Host Audits · Web Application Findings

Advanced · Saved Filters · Search by Assets · Apply

Plugin ID: is equal to 171349 × · Plugin Name: is equal to *SEoL* × · Clear All

Group By: None · Asset · Plugin

Filters

Apply

Select Filters · Clear All

171349

Plugin Name

□ 3 Vulnerabilities · Refresh · Fetched At: 04:33 PM · Grid: Basic View · Columns · 1 to 3 of 3 · Page 1 of 1

	Asset Name	IPv4 Add...	Seve...	Plugin Name	VPR	CVSSv3...	State	Scan O...	Last Se...	Actions
□	[redacted]	[redacted]	Critical	Apache Tomcat SEoL (6...		10	Active	Tenable.io	02/27/2...	⋮
□	[redacted]	[redacted]	Critical	Apache Tomcat SEoL (6...		10	New	Tenable.io	02/27/2...	⋮
□	[redacted]	[redacted]	Critical	Apache Tomcat SEoL (6...		10	Active	Tenable.io	02/27/2...	⋮

Apache Tomcat SEoL (6.0.x)

See All Details

Asset Information

NAME	[redacted]
IPV4 ADDRESS	[redacted]
OPERATING SYSTEM	Linux Kernel 3.0 on Ubuntu 12.04 (precise)
SYSTEM TYPE	general-purpose
NETWORK	Default

Additional Information

CLOUD MISCONFIGURATIONS	0

Asset Scan Information

FIRST SEEN	02/24/2022 at 05:31 PM
LAST SEEN	02/27/2023 at 04:29 AM
LAST LICENSED SCAN	02/27/2023 at 04:29 AM
SOURCE	Nessus Scan
SCAN ORIGIN	Tenable.io

Vulnerability Information

SEVERITY	Critical
PLUGIN ID	171349
PORT	8080
PROTOCOL	TCP
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSSV2 BASE SCORE	10
CVSSV2 VECTOR	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
LIVE RESULT	No

Discovery

FIRST SEEN	02/27/2023 at 04:20 AM
LAST SEEN	02/27/2023 at 02:38 PM

Overview · Plugin Output

Description

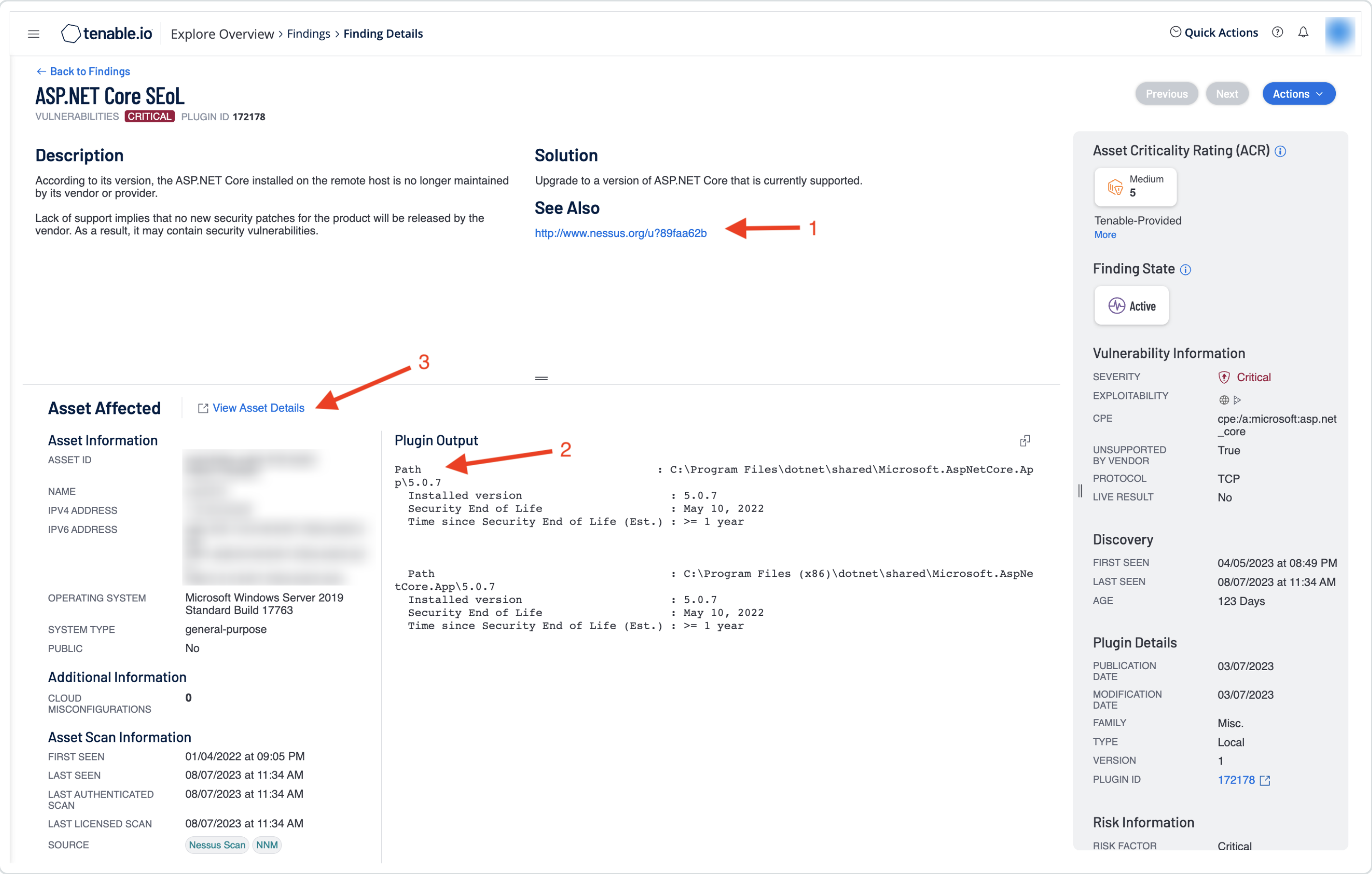
According to its version, Apache Tomcat is 6.0.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

This page contains a lot of useful information, such as a link to additional resources (**1**), the path to the out-of-date application (**2**), and details about the affected asset (**3**).



ASP.NET Core SEoL

VULNERABILITIES CRITICAL PLUGIN ID **172178**

Description

According to its version, the ASP.NET Core installed on the remote host is no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of ASP.NET Core that is currently supported.

See Also

http://www.nessus.org/u?89faa62b

Asset Affected

View Asset Details

Asset Information

ASSET ID [redacted]

NAME

IPV4 ADDRESS

IPV6 ADDRESS

OPERATING SYSTEM	Microsoft Windows Server 2019 Standard Build 17763
SYSTEM TYPE	general-purpose
PUBLIC	No

Additional Information

CLOUD MISCONFIGURATIONS	**0**

Asset Scan Information

FIRST SEEN	01/04/2022 at 09:05 PM
LAST SEEN	08/07/2023 at 11:34 AM
LAST AUTHENTICATED SCAN	08/07/2023 at 11:34 AM
LAST LICENSED SCAN	08/07/2023 at 11:34 AM
SOURCE	Nessus Scan NNM

Plugin Output

```
Path                                       : C:\Program Files\dotnet\shared\Microsoft.AspNetCore.Ap
p\5.0.7
  Installed version                          : 5.0.7
  Security End of Life                       : May 10, 2022
  Time since Security End of Life (Est.) : >= 1 year


  Path                                       : C:\Program Files (x86)\dotnet\shared\Microsoft.AspNe
tCore.App\5.0.7
  Installed version                          : 5.0.7
  Security End of Life                       : May 10, 2022
  Time since Security End of Life (Est.) : >= 1 year
```

Asset Criticality Rating (ACR)

Medium
5

Tenable-Provided
More

Finding State

Active

Vulnerability Information

SEVERITY	Critical
EXPLOITABILITY	
CPE	cpe:/a:microsoft:asp.net_core
UNSUPPORTED BY VENDOR	True
PROTOCOL	TCP
LIVE RESULT	No

Discovery

FIRST SEEN	04/05/2023 at 08:49 PM
LAST SEEN	08/07/2023 at 11:34 AM
AGE	123 Days

Plugin Details

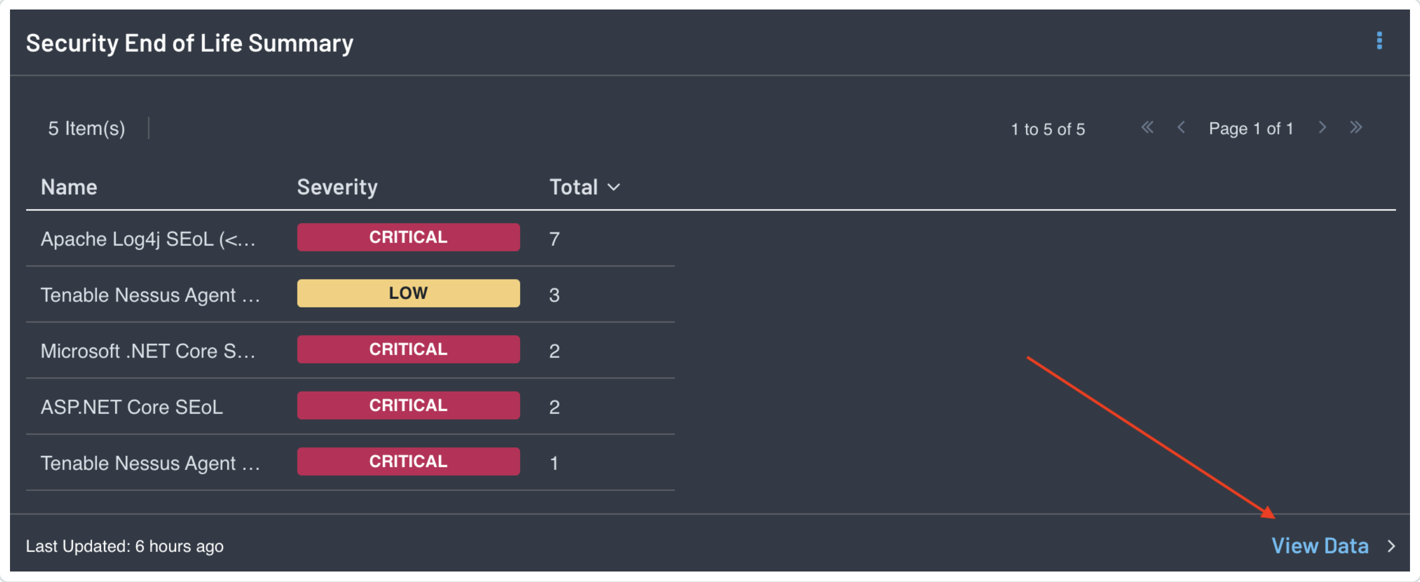
PUBLICATION DATE	03/07/2023
MODIFICATION DATE	03/07/2023
FAMILY	Misc.
TYPE	Local
VERSION	1
PLUGIN ID	172178

Risk Information

RISK FACTOR	Critical

Drill Down for Tenable Security Center

Drilling down into the data presents a vulnerability summary where additional details on each identified SEoL finding can be viewed. Click on **View Data >** to drill into the Findings page for more details and to perform refined searches.



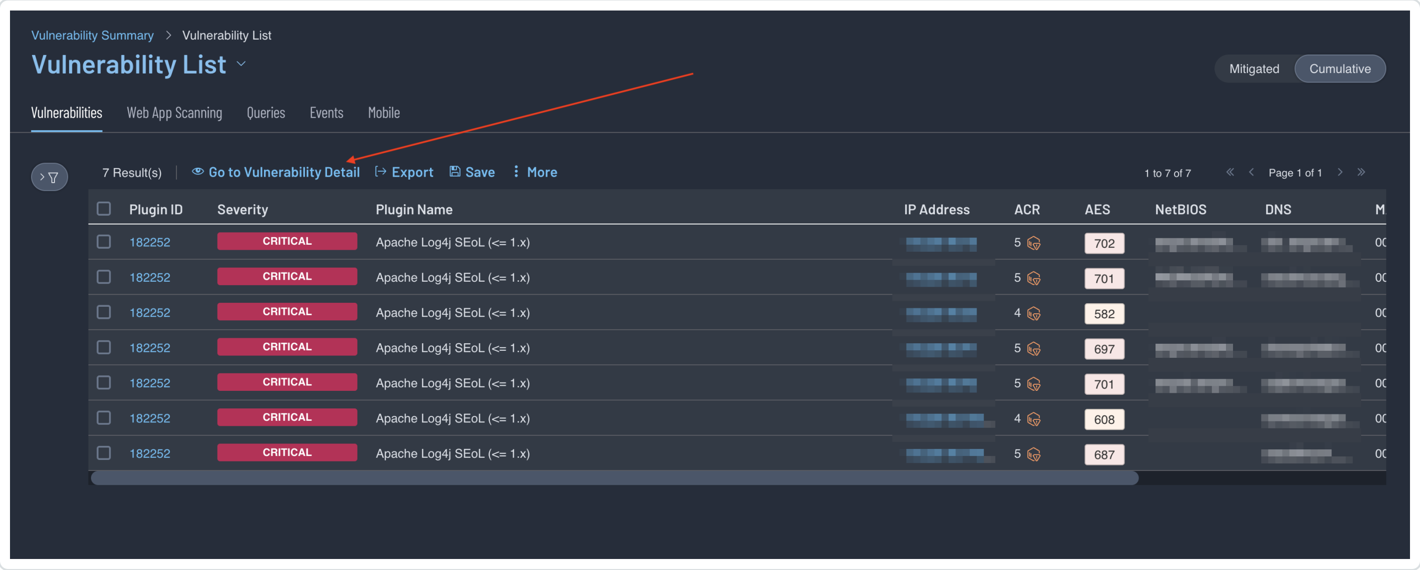
Security End of Life Summary

5 Item(s) | 1 to 5 of 5 | Page 1 of 1

Name	Severity	Total
Apache Log4j SEoL (<...	CRITICAL	7
Tenable Nessus Agent ...	LOW	3
Microsoft .NET Core S...	CRITICAL	2
ASP.NET Core SEoL	CRITICAL	2
Tenable Nessus Agent ...	CRITICAL	1

Last Updated: 6 hours ago

For more details, click on an asset (**1**) and select **Go to Vulnerability Details**.



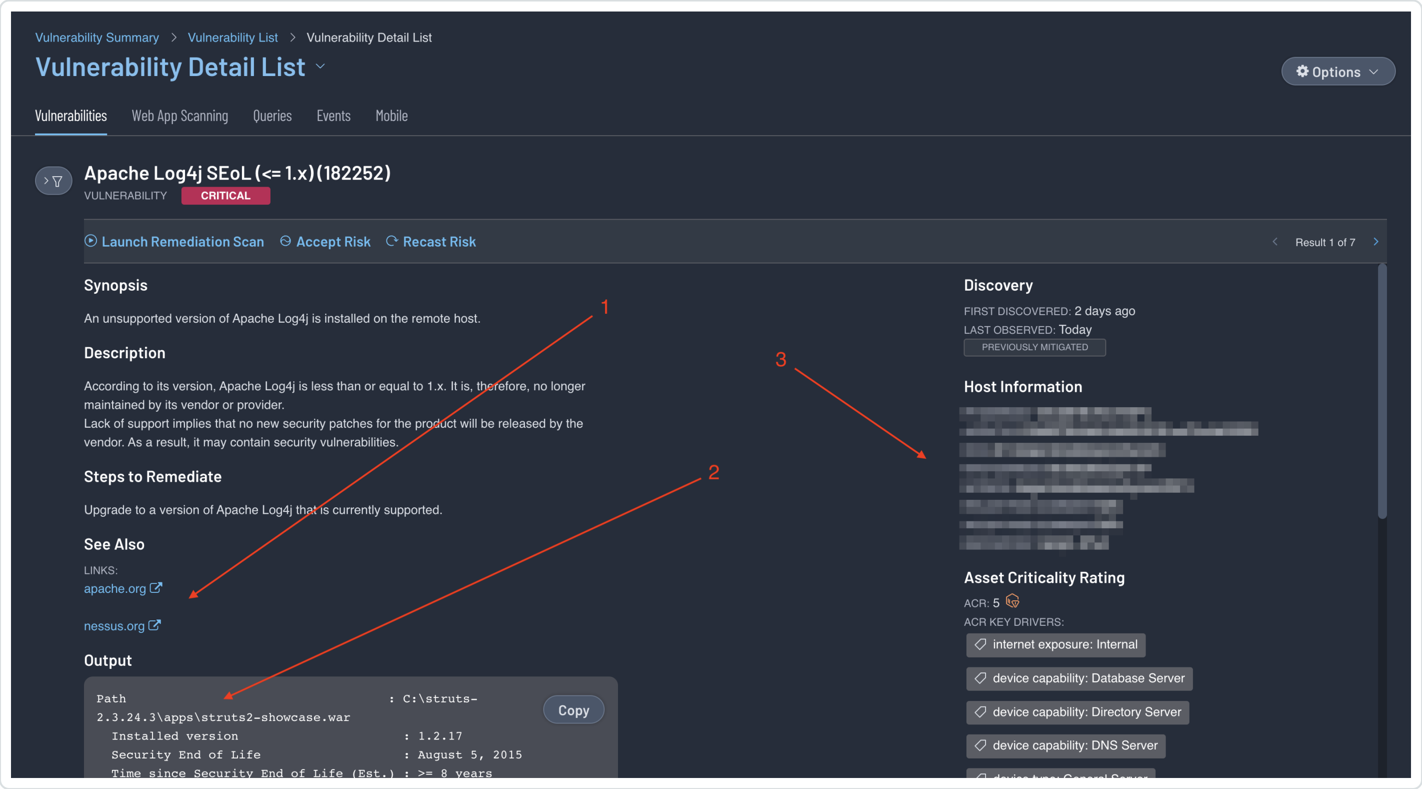
Vulnerability Summary > Vulnerability List

Vulnerability List

7 Result(s) | 1 to 7 of 7 | Page 1 of 1

□	Plugin ID	Severity	Plugin Name	IP Address	ACR	AES	NetBIOS	DNS	M
□	182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]	5	702	[redacted]	[redacted]	0
□	182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]	5	701	[redacted]	[redacted]	0
□	182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]	4	582			0
□	182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]	5	697	[redacted]	[redacted]	0
□	182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]	5	701	[redacted]	[redacted]	0
□	182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]	4	608		[redacted]	0
□	182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]	5	687		[redacted]	0

This page contains a lot of useful information, such as a link to additional resources (**1**), the path to the out-of-date application (**2**), and details about the affected asset (**3**).



Vulnerability Detail List

Apache Log4j SEoL (<= 1.x) (182252)

VULNERABILITY CRITICAL

Synopsis

An unsupported version of Apache Log4j is installed on the remote host.

Description

According to its version, Apache Log4j is less than or equal to 1.x. It is, therefore, no longer maintained by its vendor or provider.
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Steps to Remediate

Upgrade to a version of Apache Log4j that is currently supported.

See Also

LINKS:
apache.org

nessus.org

Output

```
Path                                     : C:\struts-
2.3.24.3\apps\struts2-showcase.war
  Installed version                        : 1.2.17
  Security End of Life                     : August 5, 2015
  Time since Security End of Life (Est.) : >= 8 years
```

Discovery

FIRST DISCOVERED: 2 days ago
LAST OBSERVED: Today
PREVIOUSLY MITIGATED

Host Information

[redacted]

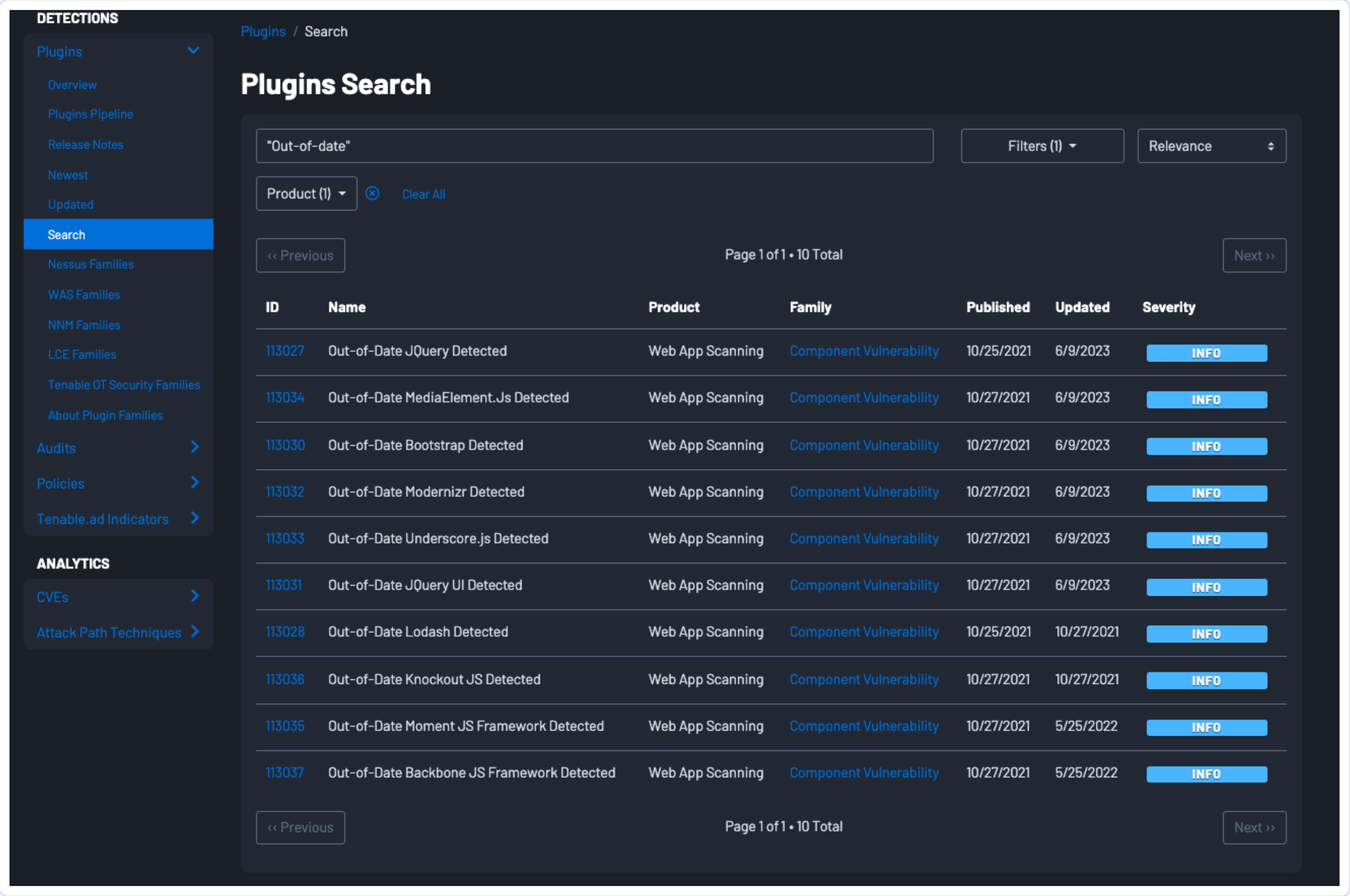
Asset Criticality Rating

ACR: 5
ACR KEY DRIVERS:

- internet exposure: Internal
- device capability: Database Server
- device capability: Directory Server
- device capability: DNS Server
- device type: General Server

Out-of-Date Libraries

The Tenable Web App Scanner also contains a number of plugins that detect out-of-date libraries.



Plugins Search

"Out-of-date"

Page 1 of 1 • 10 Total

ID	Name	Product	Family	Published	Updated	Severity
113027	Out-of-Date JQuery Detected	Web App Scanning	Component Vulnerability	10/25/2021	6/9/2023	INFO
113034	Out-of-Date MediaElement.Js Detected	Web App Scanning	Component Vulnerability	10/27/2021	6/9/2023	INFO
113030	Out-of-Date Bootstrap Detected	Web App Scanning	Component Vulnerability	10/27/2021	6/9/2023	INFO
113032	Out-of-Date Modernizr Detected	Web App Scanning	Component Vulnerability	10/27/2021	6/9/2023	INFO
113033	Out-of-Date Underscore.js Detected	Web App Scanning	Component Vulnerability	10/27/2021	6/9/2023	INFO
113031	Out-of-Date JQuery UI Detected	Web App Scanning	Component Vulnerability	10/27/2021	6/9/2023	INFO
113028	Out-of-Date Lodash Detected	Web App Scanning	Component Vulnerability	10/25/2021	10/27/2021	INFO
113036	Out-of-Date Knockout JS Detected	Web App Scanning	Component Vulnerability	10/27/2021	10/27/2021	INFO
113035	Out-of-Date Moment JS Framework Detected	Web App Scanning	Component Vulnerability	10/27/2021	5/25/2022	INFO
113037	Out-of-Date Backbone JS Framework Detected	Web App Scanning	Component Vulnerability	10/27/2021	5/25/2022	INFO

Page 1 of 1 • 10 Total

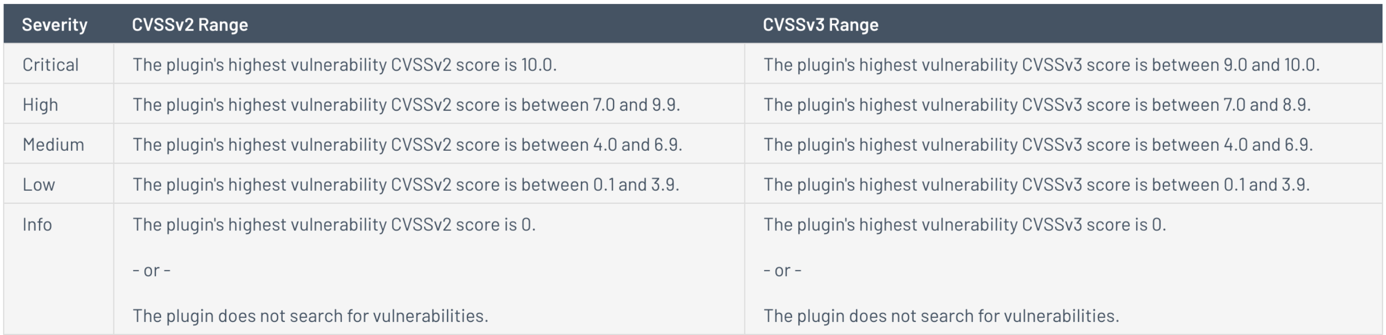
Prioritizing Vulnerabilities

Prioritizing vulnerabilities is a critical aspect of effective vulnerability management. Not all vulnerabilities pose the same risk, and limited resources may prevent organizations from addressing every vulnerability immediately. Prioritization helps focus efforts on mitigating the most critical vulnerabilities first. Here are some strategies to consider when prioritizing vulnerabilities.

Vulnerabilities by Severity

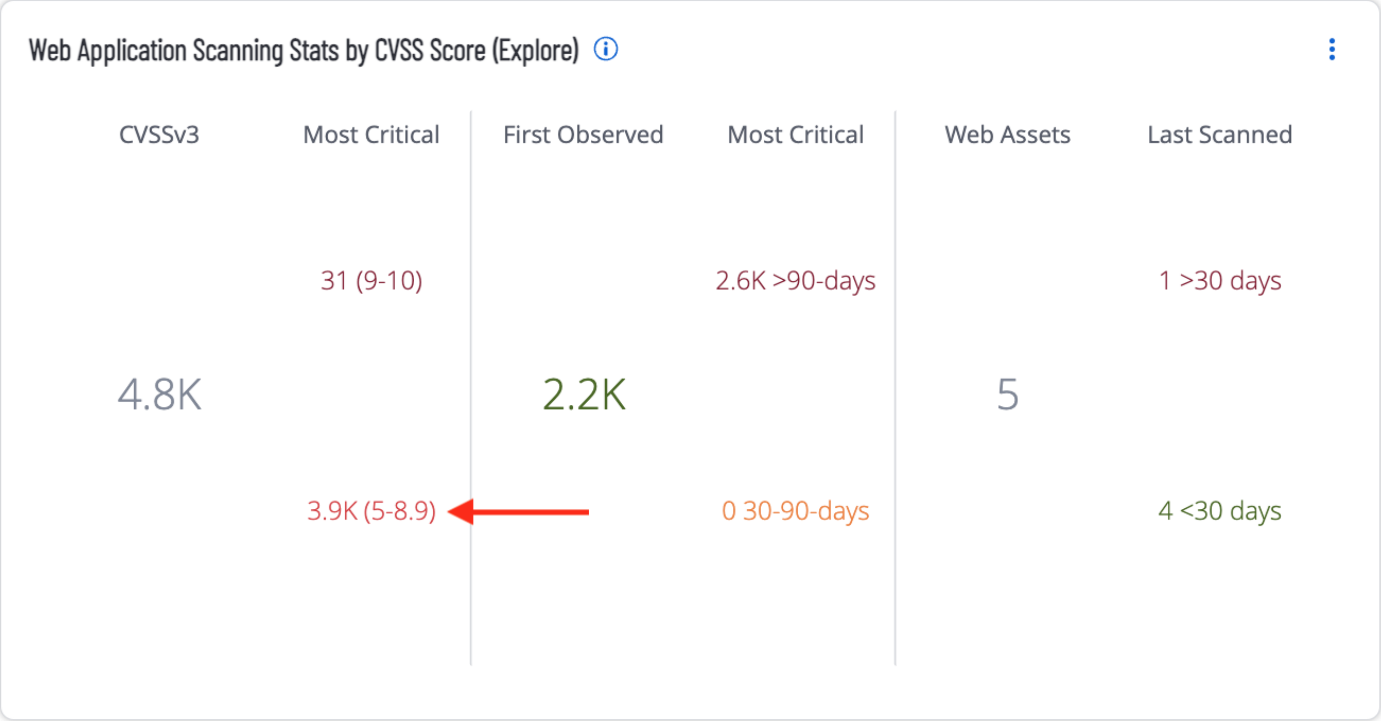
Tenable assigns all vulnerabilities a severity level (Info, Low, Medium, High, Critical) based on the vulnerabilities static CVSS score. The score used (CVSSv2 or CVSSv3) is dependent on the configuration set within Tenable Vulnerability Management. CVSSv3 is currently the default severity selection in Tenable products. For Tenable Security Center, the CVSS version is controlled by a setting for each Organization by the administrator

> **Note:** This setting does not affect Tenable Web App Scanning or Tenable Container Security vulnerabilities.



Severity	CVSSv2 Range	CVSSv3 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.	The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.	The plugin's highest vulnerability CVSSv3 score is between 7.0 and 8.9.
Medium	The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.	The plugin's highest vulnerability CVSSv3 score is between 4.0 and 6.9.
Low	The plugin's highest vulnerability CVSSv2 score is between 0.1 and 3.9.	The plugin's highest vulnerability CVSSv3 score is between 0.1 and 3.9.
Info	The plugin's highest vulnerability CVSSv2 score is 0. - or - The plugin does not search for vulnerabilities.	The plugin's highest vulnerability CVSSv3 score is 0. - or - The plugin does not search for vulnerabilities.

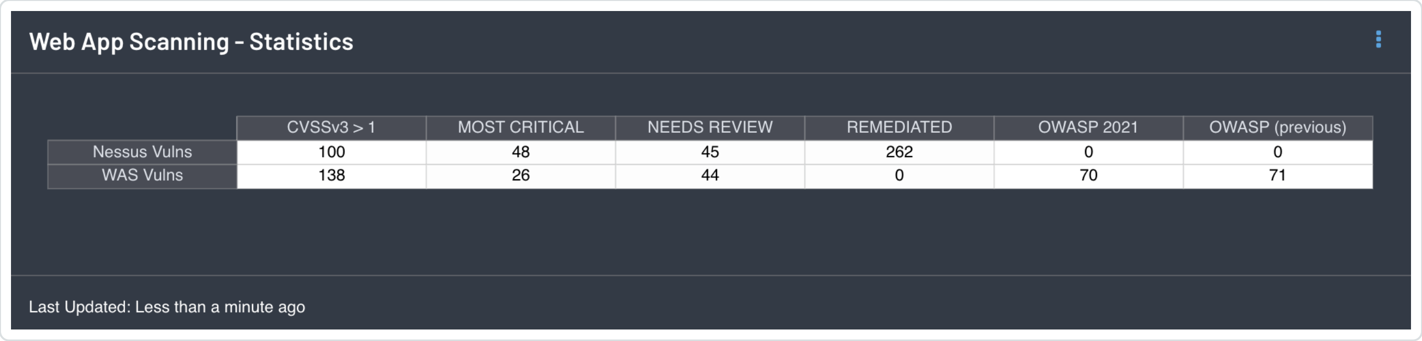
The **Web Application Scanning Stats by CVSS Score** widget displays summary counts by Severity for Tenable Web App Scanning findings. The widget highlights the Tenable Web App Scanning findings, which require the most attention, by using the severity filter to only display Medium, High, and Critical WAS findings.



Web Application Scanning Stats by CVSS Score (Explore)

CVSSv3	Most Critical	First Observed	Most Critical	Web Assets	Last Scanned
4.8K	31 (9-10) 3.9K (5-8.9)	2.2K	2.6K >90-days 0 30-90-days	5	1 >30 days 4 <30 days

The **Web App Scanning - Statistics** component for Tenable Security Center displays summary counts for Tenable Nessus and Tenable Web App Scanning findings. The component highlights the Tenable Web App Scanning findings, and Tenable Nessus scan results associated with web application plugin families (CGI abuses, and Web Servers) which require the most attention.



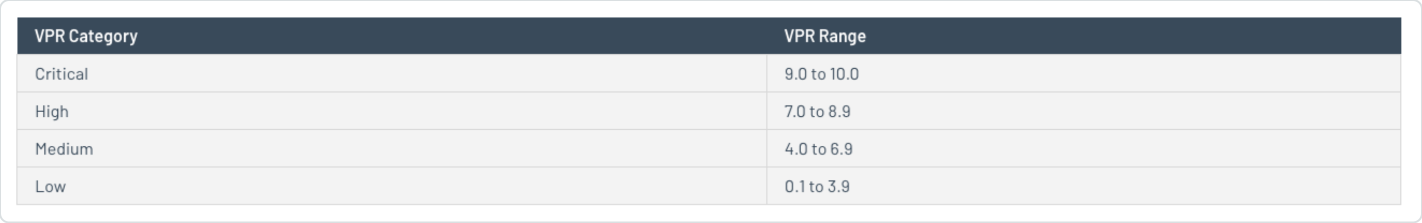
Web App Scanning - Statistics

	CVSSv3 > 1	MOST CRITICAL	NEEDS REVIEW	REMEDIATED	OWASP 2021	OWASP (previous)
Nessus Vulns	100	48	45	262	0	0
WAS Vulns	138	26	44	0	70	71

Last Updated: Less than a minute ago

Vulnerabilities by VPR

Tenable calculates a dynamic Vulnerability Priority Rating (VPR) for most vulnerabilities. VPR is a unique vulnerability severity rating in that the rating can change over time. Tenable updates a vulnerability's VPR score daily to reflect the current threat landscape. VPR ranges are values from 0.1-10, with the highest value representing a higher likelihood of exploitation.



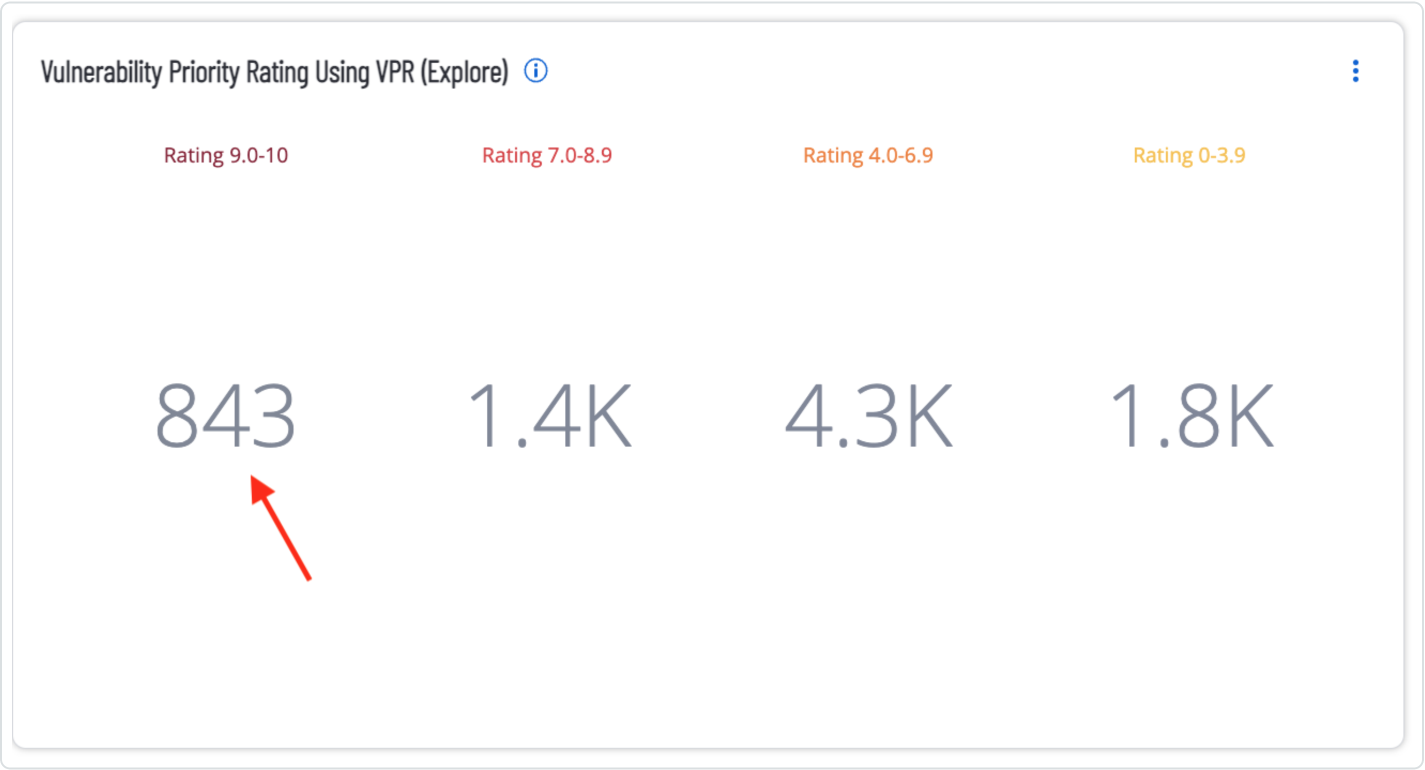
VPR Category	VPR Range
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

VPR severity ratings cannot be edited or customized. VPR scores are derived from seven key drivers:

- **Age of Vulnerability:** - The number of days since the National Vulnerability Database (NVD) published the vulnerability.
- **CVSSv3 Impact Score** - The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Vulnerability Management displays a Tenable-predicted score.

- **Exploit Code Maturity** - The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (High, Functional, PoC, or Unproven) parallel the CVSS Exploit Code Maturity categories.
- **Product Coverage** - The relative number of unique products affected by the vulnerability: Low, Medium, High, or Very High.
- **Threat Sources** - A list of all sources (e.g., social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays No recorded events.
- **Threat Intensity** - The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability: Very Low, Low, Medium, High, or Very High.
- **Threat Recency** - The number of days (0-180) since a threat event occurred for the vulnerability.

The **Vulnerability Priority Rating Using VPR** widget for Tenable Vulnerability Management displays the vulnerability count, organized by Vulnerability Priority Rating (VPR) category from the traditional vulnerability scans collected using Nessus scanners. VPR is a dynamic metric representing the likelihood of a vulnerability being exploited and its severity. Tenable recommends remediating vulnerabilities with a higher VPR first.

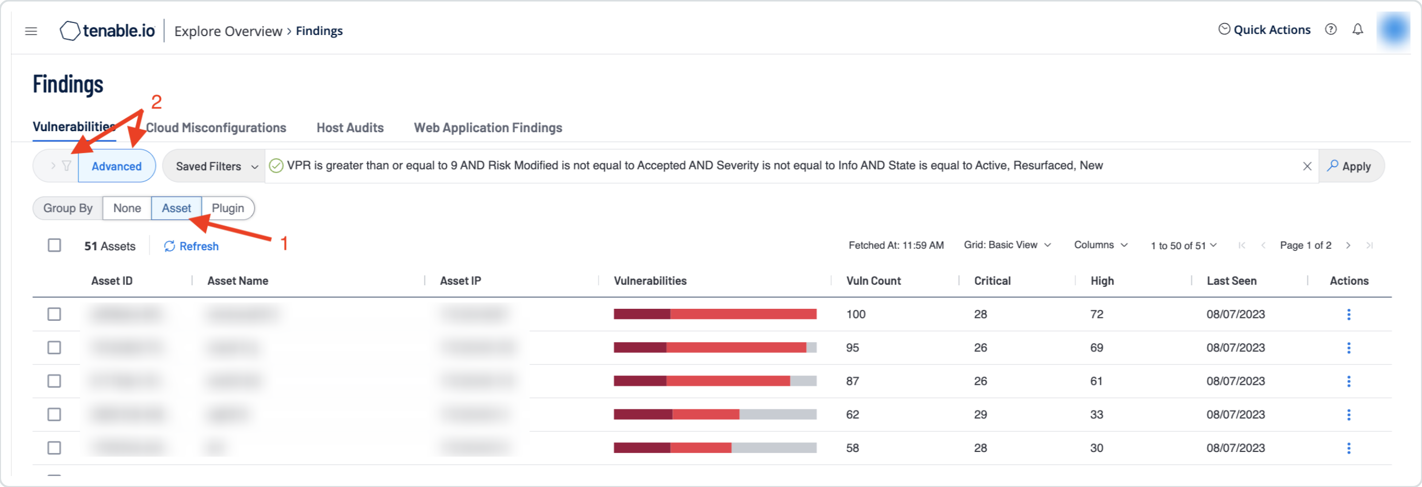


Vulnerability Priority Rating Using VPR (Explore)

Rating 9.0-10	Rating 7.0-8.9	Rating 4.0-6.9	Rating 0-3.9
843	1.4K	4.3K	1.8K

Drilling Down in Tenable Vulnerability Management

Drilling down in the widget enables a more refined search, based on specified conditions. To display all assets with a VPR rating of 9.0-10, click on the summary button, shown in the image above. The findings can be sorted by **Asset** (**1**) and more filters can be applied by clicking on the **Advanced** filter (**2**).

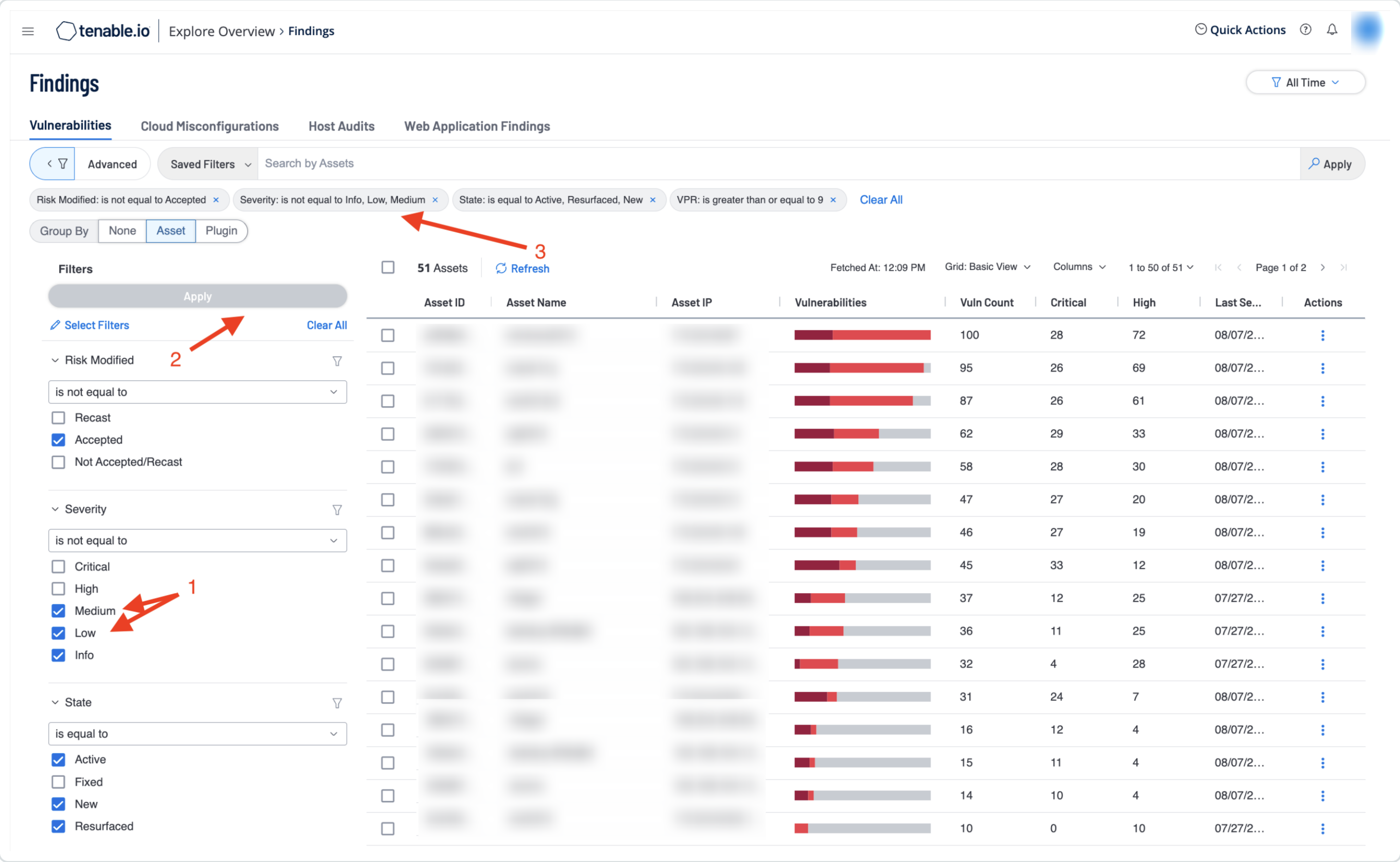


VPR is greater than or equal to 9 AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New

51 Assets

	Asset ID	Asset Name	Asset IP	Vulnerabilities	Vuln Count	Critical	High	Last Seen	Actions
□	[redacted]	[redacted]	[redacted]		100	28	72	08/07/2023	⋮
□	[redacted]	[redacted]	[redacted]		95	26	69	08/07/2023	⋮
□	[redacted]	[redacted]	[redacted]		87	26	61	08/07/2023	⋮
□	[redacted]	[redacted]	[redacted]		62	29	33	08/07/2023	⋮
□	[redacted]	[redacted]	[redacted]		58	28	30	08/07/2023	⋮

For example, to only display assets having vulnerabilities with a VPR greater than or equal to 9 and a CVSS score of Critical and High, filter out the Medium and Low CVSS vulnerabilities by checking the boxes under Severity "is not equal to" (**1**), and click on Apply (**2**). The Medium and Low severity vulnerabilities are now filtered out (**3**).



Findings

Risk Modified: is not equal to Accepted ×   Severity: is not equal to Info, Low, Medium ×   State: is equal to Active, Resurfaced, New ×   VPR: is greater than or equal to 9 ×

Risk Modified
is not equal to
- □ Recast
- ☑ Accepted
- □ Not Accepted/Recast

Severity
is not equal to
- □ Critical
- □ High
- ☑ Medium
- ☑ Low
- ☑ Info

State
is equal to
- ☑ Active
- □ Fixed
- ☑ New
- ☑ Resurfaced

51 Assets   Refresh   Fetched At: 12:09 PM   Grid: Basic View   Columns   1 to 50 of 51   Page 1 of 2

Asset ID	Asset Name	Asset IP	Vulnerabilities	Vuln Count	Critical	High	Last Se...	Actions
[redacted]	[redacted]	[redacted]		100	28	72	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		95	26	69	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		87	26	61	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		62	29	33	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		58	28	30	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		47	27	20	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		46	27	19	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		45	33	12	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		37	12	25	07/27/2...	⋮
[redacted]	[redacted]	[redacted]		36	11	25	07/27/2...	⋮
[redacted]	[redacted]	[redacted]		32	4	28	07/27/2...	⋮
[redacted]	[redacted]	[redacted]		31	24	7	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		16	12	4	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		15	11	4	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		14	10	4	08/07/2...	⋮
[redacted]	[redacted]	[redacted]		10	0	10	07/27/2...	⋮

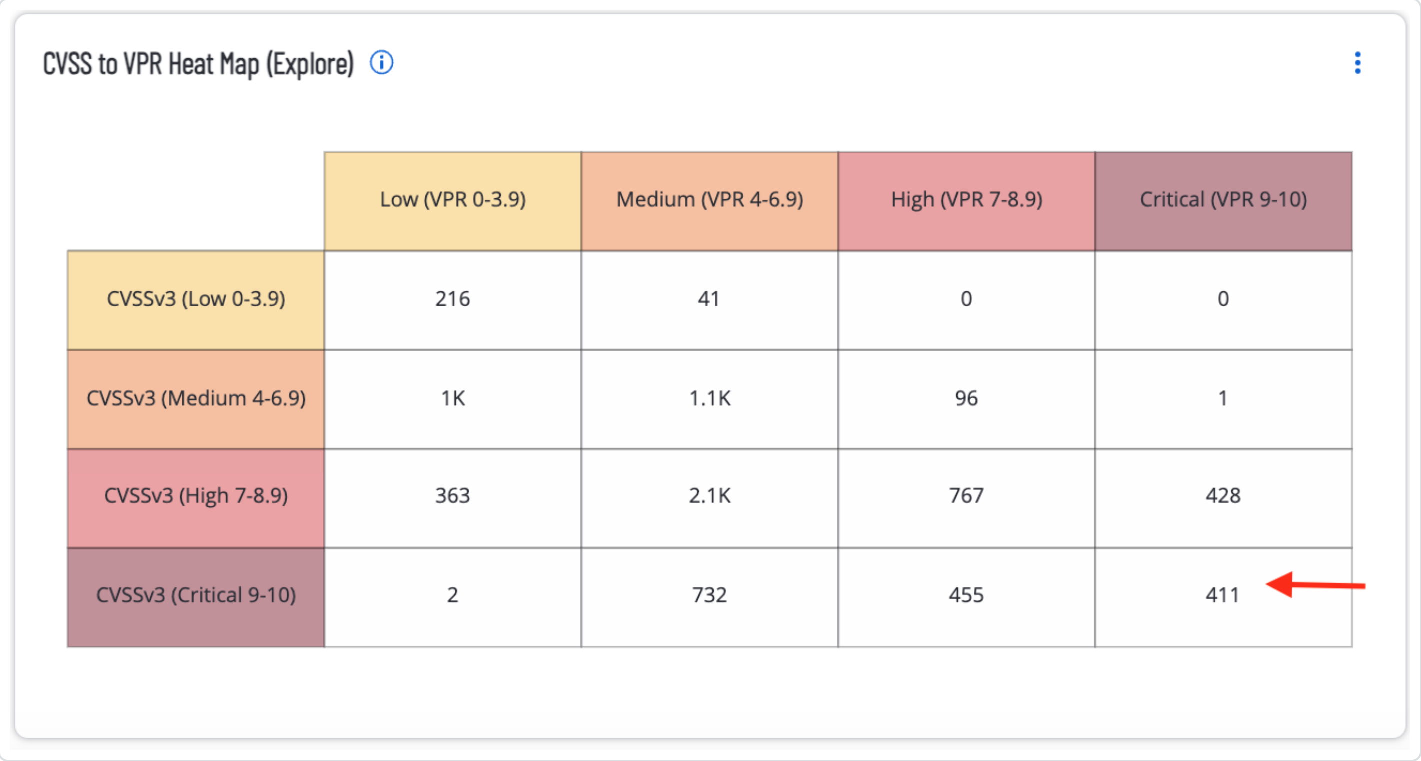
Vulnerabilities by CVSS

The Common Vulnerability Scoring System (CVSS) is a metric from 0 to 10 assigned by the product vendor or the National Vulnerability Database (NVD) to indicate the severity of a vulnerability. CVSS scores are produced by the entity or organization producing and maintaining the product or a third party scoring on their behalf. CVSS Base Scores alone are not a measure of business risk nor do CVSS values account for real-world risk or asset criticality within an organization's specific environment as scores are not likely to change once published.

Tenable recommends supplementing CVSS Base Scores with another temporal or environmental score to more accurately measure severity and rank threats. Such factors may include the risk of monetary loss due to breach, risks of damage or threat to life or property.

The **CVSS to VPR Heat Map (Explore)** widget provides a correlation between CVSSv3 scores and Vulnerability Priority Rating (VPR) scoring for the vulnerabilities present in the organization. Each cell consists of a combination of cross-mapping of CVSS and VPR scoring. Using a heat map approach, the filters begin in the left upper corner with vulnerabilities that present least risk.

Moving to the right and lower down the matrix the colors change darker from yellow to red as the risk levels increase. Click on the cell in the lower right corner of the widget to drill down into details about the most critical CVSSv3 and VPR vulnerabilities.

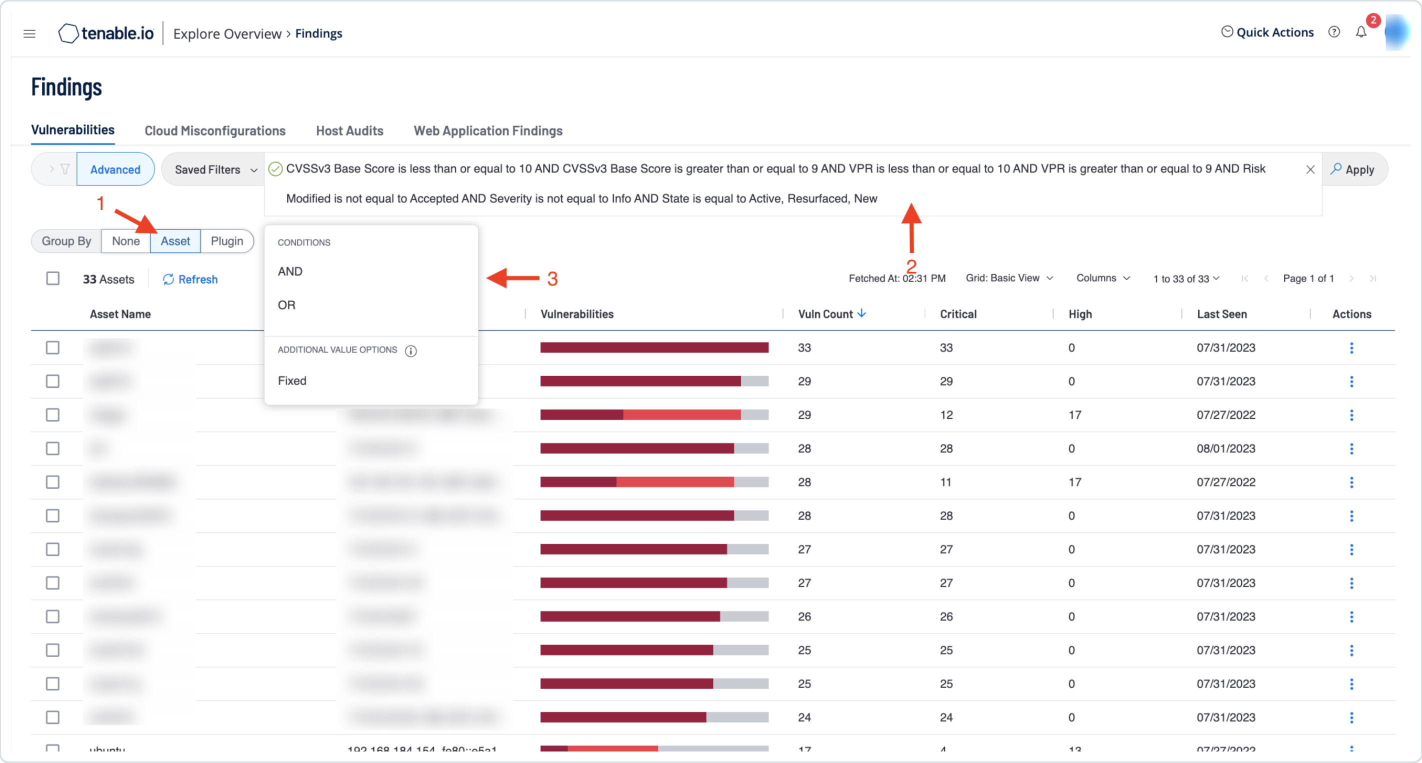


CVSS to VPR Heat Map (Explore)

	Low (VPR 0-3.9)	Medium (VPR 4-6.9)	High (VPR 7-8.9)	Critical (VPR 9-10)
CVSSv3 (Low 0-3.9)	216	41	0	0
CVSSv3 (Medium 4-6.9)	1K	1.1K	96	1
CVSSv3 (High 7-8.9)	363	2.1K	767	428
CVSSv3 (Critical 9-10)	2	732	455	411

Drilling Down in Tenable Vulnerability Management

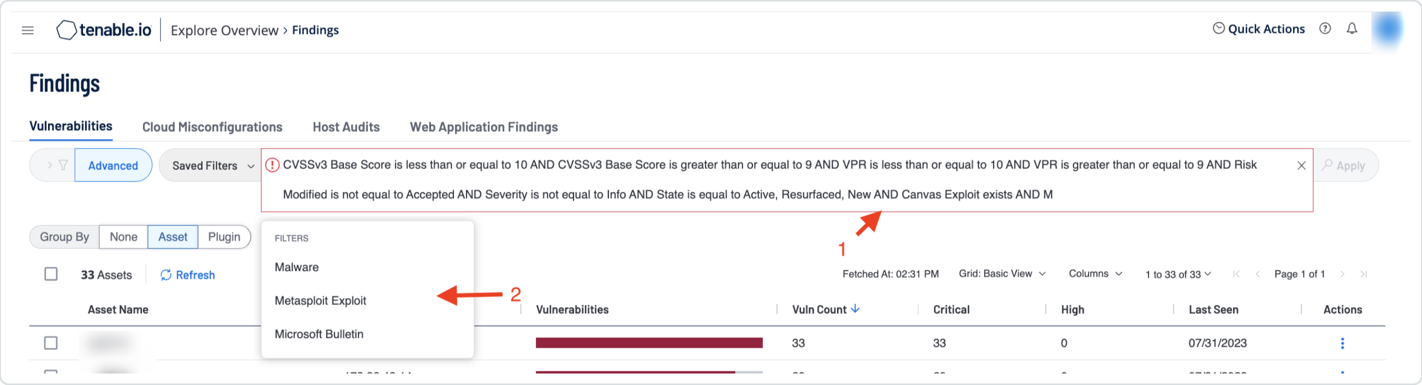
Clicking on any cell displays a Findings page with more details about the vulnerabilities in this category. For this example, the Findings are sorted by **Asset** (**1**). The filter used in the search is displayed in the center conditions field (**2**). Clicking on this field enables users to add additional Conditions (**3**).



CVSSv3 Base Score is less than or equal to 10 AND CVSSv3 Base Score is greater than or equal to 9 AND VPR is less than or equal to 10 AND VPR is greater than or equal to 9 AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New

□	Asset Name		Vulnerabilities	Vuln Count	Critical	High	Last Seen	Actions
□	[redacted]			33	33	0	07/31/2023	⋮
□	[redacted]			29	29	0	07/31/2023	⋮
□	[redacted]	[redacted]		29	12	17	07/27/2022	⋮
□	[redacted]	[redacted]		28	28	0	08/01/2023	⋮
□	[redacted]	[redacted]		28	11	17	07/27/2022	⋮
□	[redacted]	[redacted]		28	28	0	07/31/2023	⋮
□	[redacted]	[redacted]		27	27	0	07/31/2023	⋮
□	[redacted]	[redacted]		27	27	0	07/31/2023	⋮
□	[redacted]	[redacted]		26	26	0	07/31/2023	⋮
□	[redacted]	[redacted]		25	25	0	07/31/2023	⋮
□	[redacted]	[redacted]		25	25	0	07/31/2023	⋮
□	[redacted]	[redacted]		24	24	0	07/31/2023	⋮
□	ubuntu	192.168.184.154, fe80::e5a1		17	4	13	07/27/2022	⋮

For example, users may want to see if any of the vulnerabilities in this category can be exploited through the Metaploit or Canvas frameworks. As shown in the following image, select the "**AND**" condition from the Conditions menu (**1**) and start typing the desired Conditions until they are displayed and can be selected (**2**). In the following example, the "**AND**" condition is selected, followed by "**Canvas Exploit**," then "**exists**," followed by "**Metasploit Exploit**."



≡ tenable.io | Explore Overview › Findings — Quick Actions

Findings

Vulnerabilities | Cloud Misconfigurations | Host Audits | Web Application Findings

Advanced | Saved Filters ⌄ | ⓘ CVSSv3 Base Score is less than or equal to 10 AND CVSSv3 Base Score is greater than or equal to 9 AND VPR is less than or equal to 10 AND VPR is greater than or equal to 9 AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New AND Canvas Exploit exists AND M × | Apply

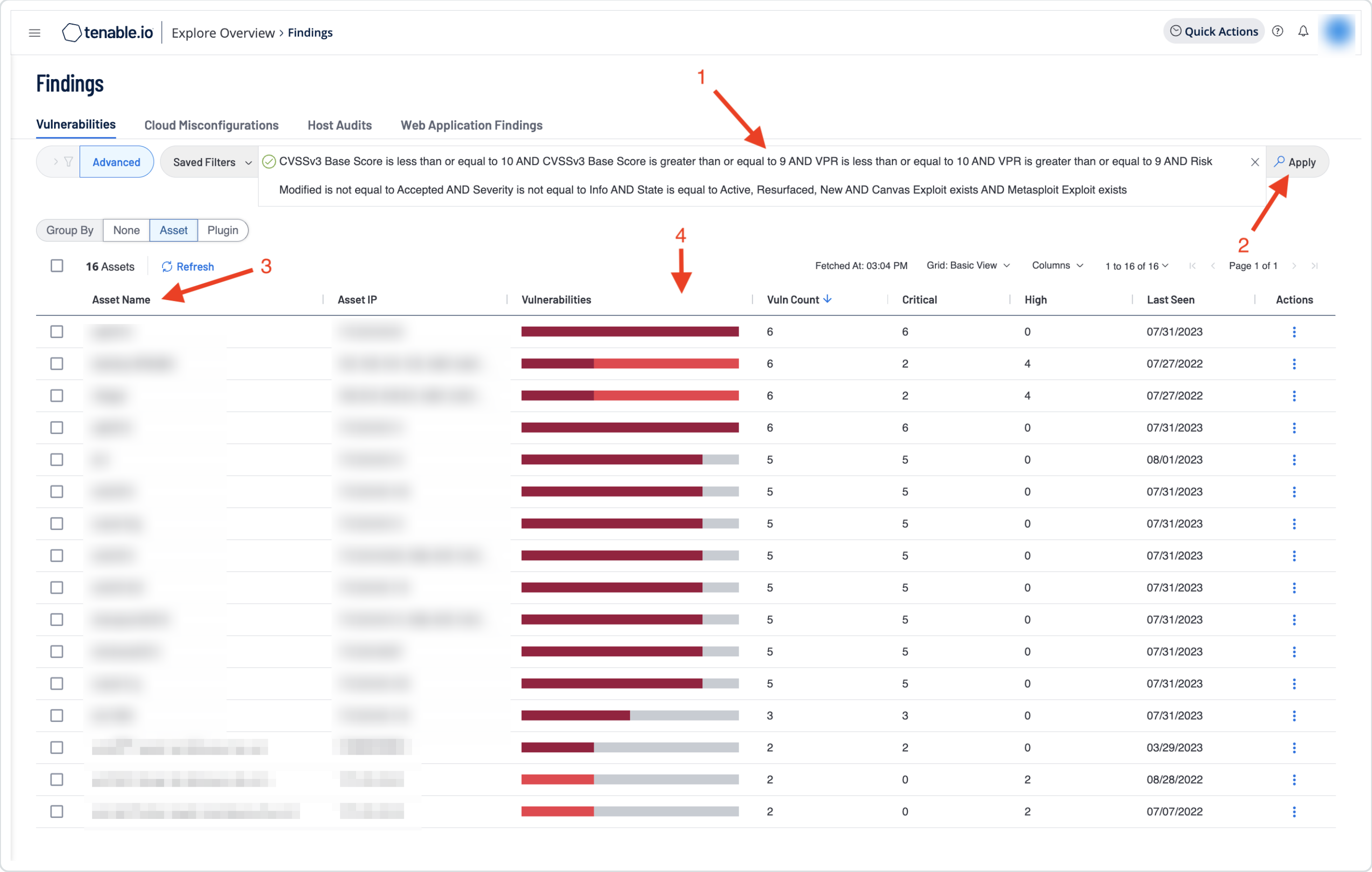
Group By: None | **Asset** | Plugin

FILTERS
- Malware
- Metasploit Exploit
- Microsoft Bulletin

□ 33 Assets | Refresh — Fetched At: 02:31 PM | Grid: Basic View ⌄ | Columns ⌄ | 1 to 33 of 33 ⌄ | Page 1 of 1

	Asset Name	Vulnerabilities	Vuln Count ↓	Critical	High	Last Seen	Actions
□	[redacted]		33	33	0	07/31/2023	⋮

The full search is shown in the following image (**1**). Click on Apply (**2**) to search for these conditions. The results are then displayed, sorted by the Asset Name (**3**) with the greatest number of vulnerabilities (**4**) that meet the specified conditions in the filter search.



≡ tenable.io | Explore Overview › Findings — Quick Actions

Findings

Vulnerabilities | Cloud Misconfigurations | Host Audits | Web Application Findings

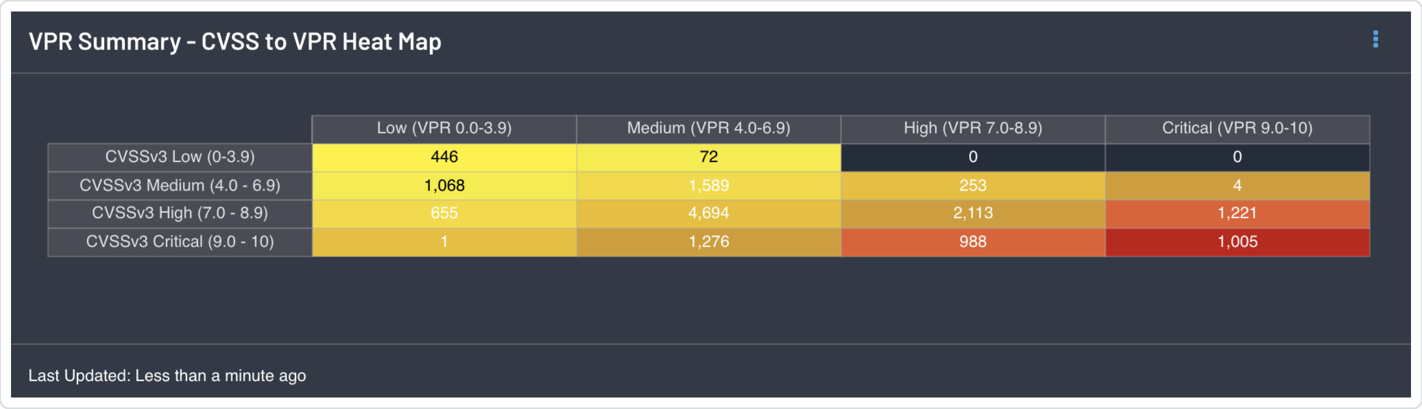
Advanced | Saved Filters ⌄ | ✓ CVSSv3 Base Score is less than or equal to 10 AND CVSSv3 Base Score is greater than or equal to 9 AND VPR is less than or equal to 10 AND VPR is greater than or equal to 9 AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New AND Canvas Exploit exists AND Metasploit Exploit exists × | Apply

Group By: None | **Asset** | Plugin

□ 16 Assets | Refresh — Fetched At: 03:04 PM | Grid: Basic View ⌄ | Columns ⌄ | 1 to 16 of 16 ⌄ | Page 1 of 1

	Asset Name	Asset IP	Vulnerabilities	Vuln Count ↓	Critical	High	Last Seen	Actions
□	[redacted]	[redacted]		6	6	0	07/31/2023	⋮
□	[redacted]	[redacted]		6	2	4	07/27/2022	⋮
□	[redacted]	[redacted]		6	2	4	07/27/2022	⋮
□	[redacted]	[redacted]		6	6	0	07/31/2023	⋮
□	[redacted]	[redacted]		5	5	0	08/01/2023	⋮
□	[redacted]	[redacted]		5	5	0	07/31/2023	⋮
□	[redacted]	[redacted]		5	5	0	07/31/2023	⋮
□	[redacted]	[redacted]		5	5	0	07/31/2023	⋮
□	[redacted]	[redacted]		5	5	0	07/31/2023	⋮
□	[redacted]	[redacted]		5	5	0	07/31/2023	⋮
□	[redacted]	[redacted]		5	5	0	07/31/2023	⋮
□	[redacted]	[redacted]		5	5	0	07/31/2023	⋮
□	[redacted]	[redacted]		3	3	0	07/31/2023	⋮
□	[redacted]	[redacted]		2	2	0	03/29/2023	⋮
□	[redacted]	[redacted]		2	0	2	08/28/2022	⋮
□	[redacted]	[redacted]		2	0	2	07/07/2022	⋮

The Tenable Security Center component, as shown below, is similar in layout.



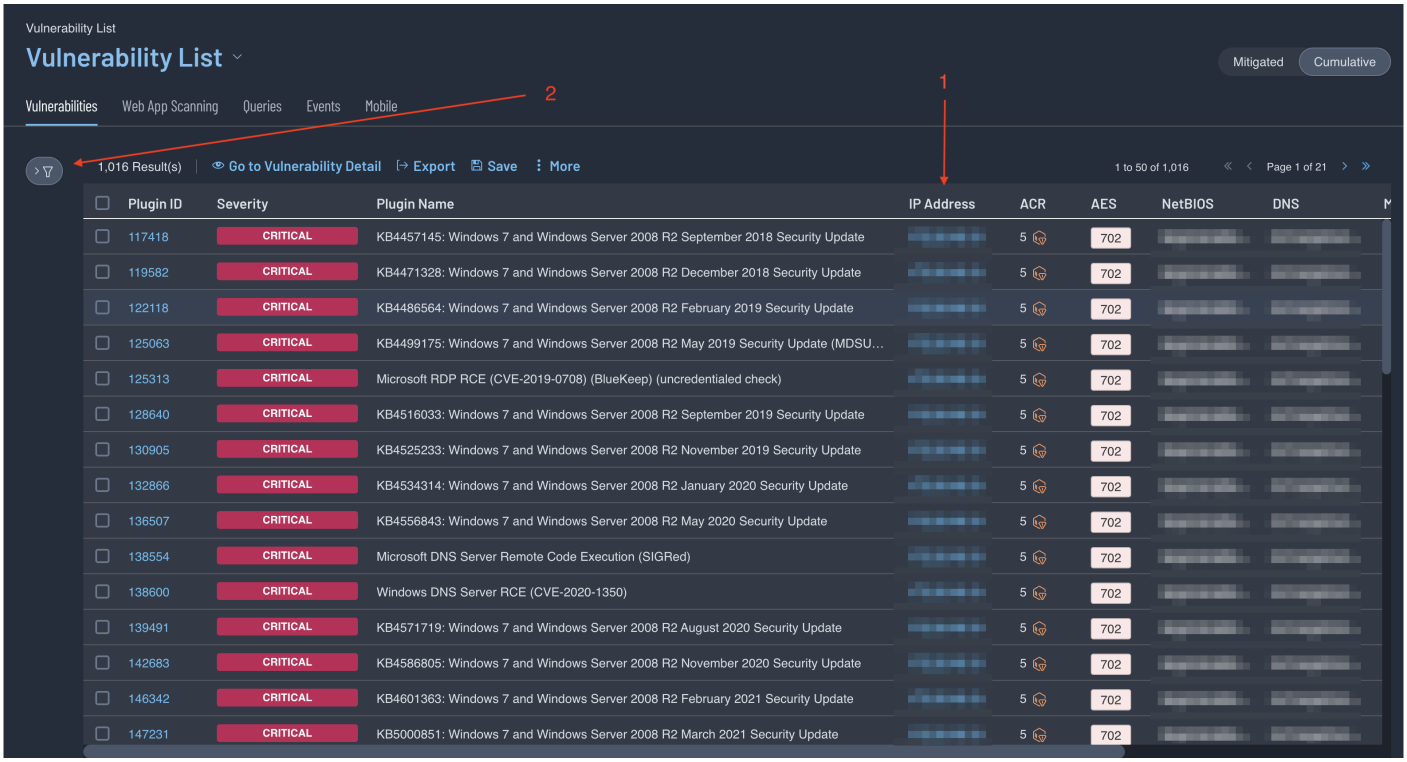
VPR Summary - CVSS to VPR Heat Map

	Low (VPR 0.0-3.9)	Medium (VPR 4.0-6.9)	High (VPR 7.0-8.9)	Critical (VPR 9.0-10)
CVSSv3 Low (0-3.9)	446	72	0	0
CVSSv3 Medium (4.0 - 6.9)	1,068	1,589	253	4
CVSSv3 High (7.0 - 8.9)	655	4,694	2,113	1,221
CVSSv3 Critical (9.0 - 10)	1	1,276	988	1,005

Last Updated: Less than a minute ago

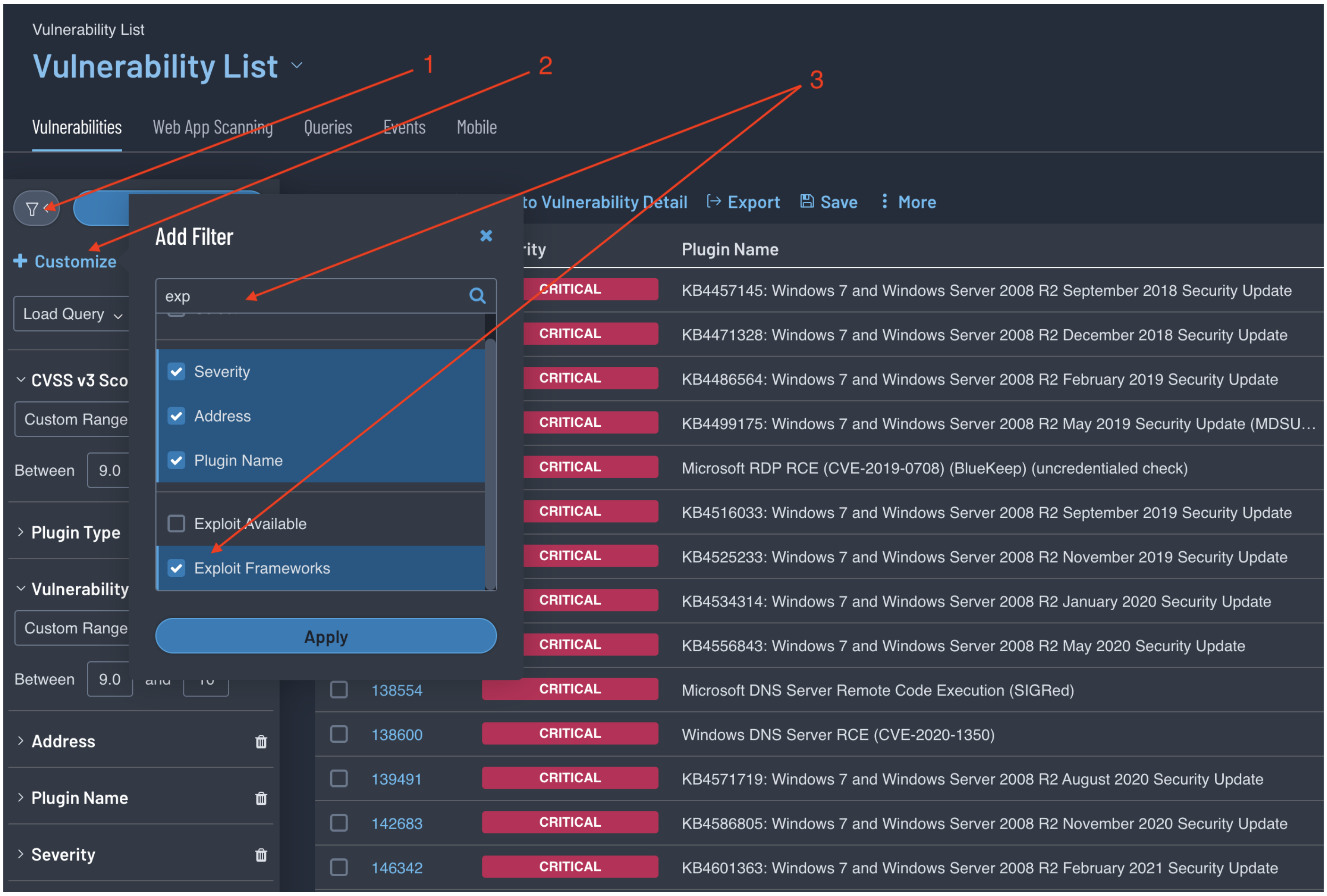
Drilling Down in Tenable Security Center

Clicking on any cell displays a Vulnerability Analysis page with more details about the vulnerabilities in this category. For this example, the Vulnerabilities will be sorted by **IP Address (1)**. The filter used in the search is only displayed in the **Filter** field (**2**). Clicking on this field enables users to add additional Filters.



Plugin ID	Severity	Plugin Name	IP Address	ACR	AES	NetBIOS	DNS
117418	CRITICAL	KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update	[redacted]	5	702	[redacted]	[redacted]
119582	CRITICAL	KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update	[redacted]	5	702	[redacted]	[redacted]
122118	CRITICAL	KB4486564: Windows 7 and Windows Server 2008 R2 February 2019 Security Update	[redacted]	5	702	[redacted]	[redacted]
125063	CRITICAL	KB4499175: Windows 7 and Windows Server 2008 R2 May 2019 Security Update (MDSU…	[redacted]	5	702	[redacted]	[redacted]
125313	CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	[redacted]	5	702	[redacted]	[redacted]
128640	CRITICAL	KB4516033: Windows 7 and Windows Server 2008 R2 September 2019 Security Update	[redacted]	5	702	[redacted]	[redacted]
130905	CRITICAL	KB4525233: Windows 7 and Windows Server 2008 R2 November 2019 Security Update	[redacted]	5	702	[redacted]	[redacted]
132866	CRITICAL	KB4534314: Windows 7 and Windows Server 2008 R2 January 2020 Security Update	[redacted]	5	702	[redacted]	[redacted]
136507	CRITICAL	KB4556843: Windows 7 and Windows Server 2008 R2 May 2020 Security Update	[redacted]	5	702	[redacted]	[redacted]
138554	CRITICAL	Microsoft DNS Server Remote Code Execution (SIGRed)	[redacted]	5	702	[redacted]	[redacted]
138600	CRITICAL	Windows DNS Server RCE (CVE-2020-1350)	[redacted]	5	702	[redacted]	[redacted]
139491	CRITICAL	KB4571719: Windows 7 and Windows Server 2008 R2 August 2020 Security Update	[redacted]	5	702	[redacted]	[redacted]
142683	CRITICAL	KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update	[redacted]	5	702	[redacted]	[redacted]
146342	CRITICAL	KB4601363: Windows 7 and Windows Server 2008 R2 February 2021 Security Update	[redacted]	5	702	[redacted]	[redacted]
147231	CRITICAL	KB5000851: Windows 7 and Windows Server 2008 R2 March 2021 Security Update	[redacted]	5	702	[redacted]	[redacted]

For example, users may want to see if any of the vulnerabilities in this category can be exploited through the Metaploit frameworks. As shown in the image below, select the filter icon (**1**) and select + Customize (**2**). In the Add Filter search area type “**exp**” to identify the Exploit Available Filter and check the box and click Apply (**3**).



CVSS v3 Sco
Custom Range
Between 9.0

Plugin Type

Vulnerability
Custom Range
Between 9.0 and 10

Address

Plugin Name

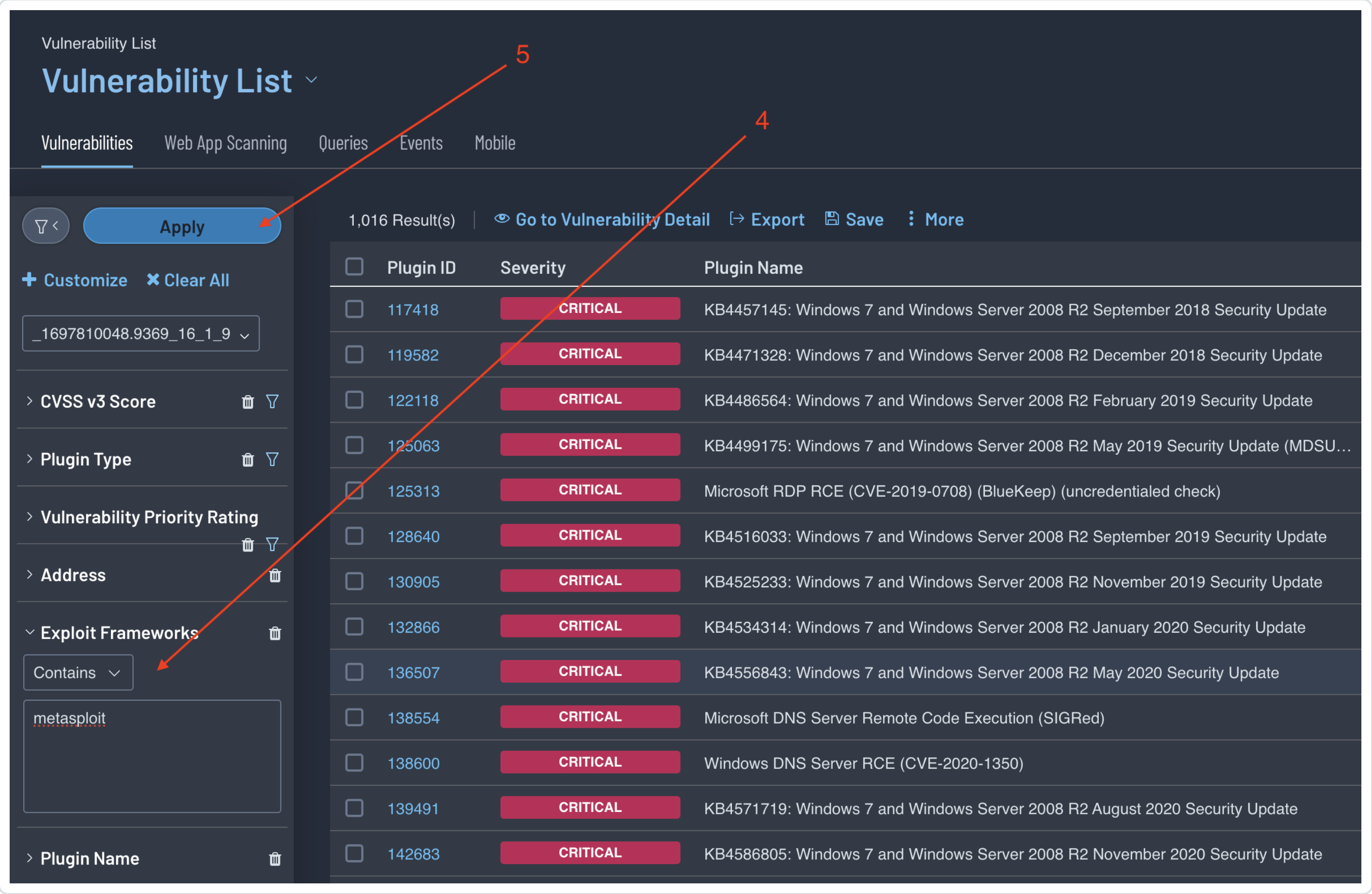
Severity

exp

☑ Severity
☑ Address
☑ Plugin Name
□ Exploit Available
☑ Exploit Frameworks

		rity	Plugin Name
		CRITICAL	KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update
		CRITICAL	KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update
		CRITICAL	KB4486564: Windows 7 and Windows Server 2008 R2 February 2019 Security Update
		CRITICAL	KB4499175: Windows 7 and Windows Server 2008 R2 May 2019 Security Update (MDSU…
		CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
		CRITICAL	KB4516033: Windows 7 and Windows Server 2008 R2 September 2019 Security Update
		CRITICAL	KB4525233: Windows 7 and Windows Server 2008 R2 November 2019 Security Update
		CRITICAL	KB4534314: Windows 7 and Windows Server 2008 R2 January 2020 Security Update
		CRITICAL	KB4556843: Windows 7 and Windows Server 2008 R2 May 2020 Security Update
□	138554	CRITICAL	Microsoft DNS Server Remote Code Execution (SIGRed)
□	138600	CRITICAL	Windows DNS Server RCE (CVE-2020-1350)
□	139491	CRITICAL	KB4571719: Windows 7 and Windows Server 2008 R2 August 2020 Security Update
□	142683	CRITICAL	KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update
□	146342	CRITICAL	KB4601363: Windows 7 and Windows Server 2008 R2 February 2021 Security Update

From the filters, find the Exploit Frameworks filter that was just added and change the drop down to “Contains” and type “metasploit” in the text area (4). Click apply (5).



_1697810048.9369_16_1_9

- CVSS v3 Score
- Plugin Type
- Vulnerability Priority Rating
- Address
- Exploit Frameworks: Contains — metasploit
- Plugin Name

1,016 Result(s)

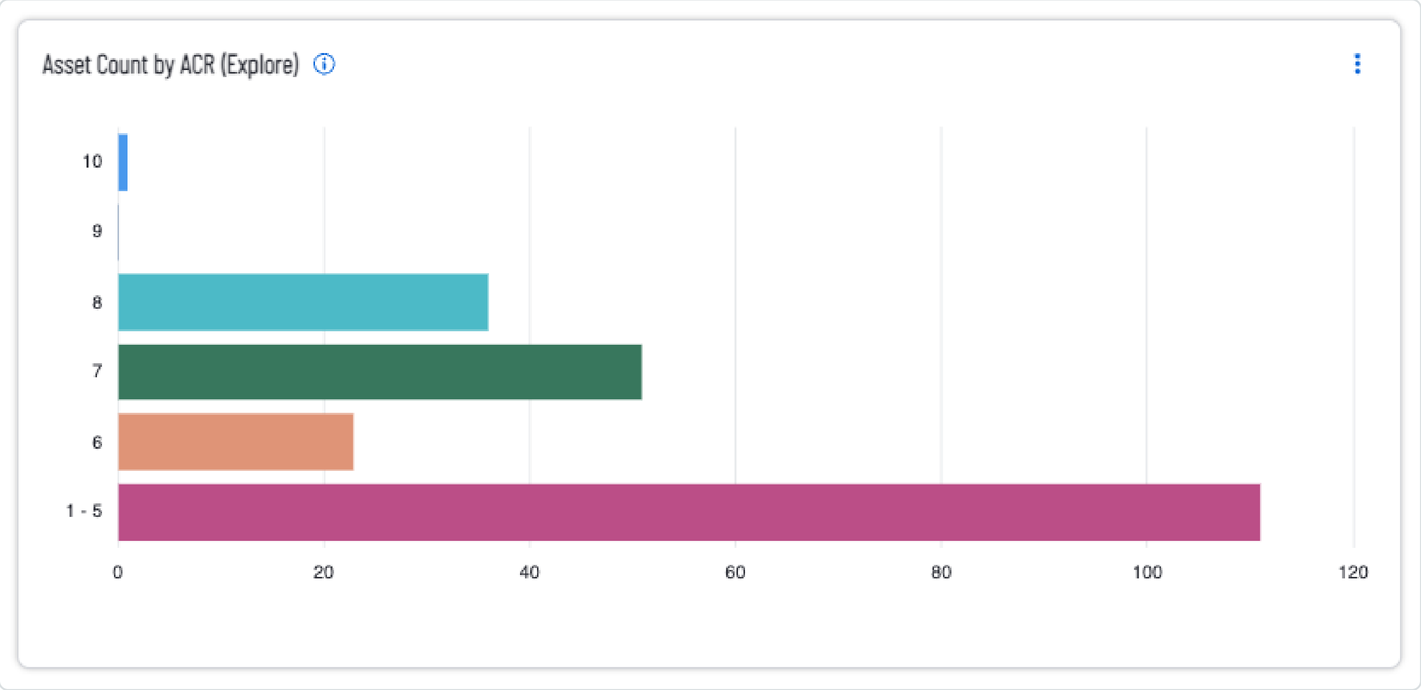
Plugin ID	Severity	Plugin Name
117418	CRITICAL	KB4457145: Windows 7 and Windows Server 2008 R2 September 2018 Security Update
119582	CRITICAL	KB4471328: Windows 7 and Windows Server 2008 R2 December 2018 Security Update
122118	CRITICAL	KB4486564: Windows 7 and Windows Server 2008 R2 February 2019 Security Update
125063	CRITICAL	KB4499175: Windows 7 and Windows Server 2008 R2 May 2019 Security Update (MDSU…
125313	CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
128640	CRITICAL	KB4516033: Windows 7 and Windows Server 2008 R2 September 2019 Security Update
130905	CRITICAL	KB4525233: Windows 7 and Windows Server 2008 R2 November 2019 Security Update
132866	CRITICAL	KB4534314: Windows 7 and Windows Server 2008 R2 January 2020 Security Update
136507	CRITICAL	KB4556843: Windows 7 and Windows Server 2008 R2 May 2020 Security Update
138554	CRITICAL	Microsoft DNS Server Remote Code Execution (SIGRed)
138600	CRITICAL	Windows DNS Server RCE (CVE-2020-1350)
139491	CRITICAL	KB4571719: Windows 7 and Windows Server 2008 R2 August 2020 Security Update
142683	CRITICAL	KB4586805: Windows 7 and Windows Server 2008 R2 November 2020 Security Update

The results that are returned will only include vulnerabilities that include Metasploit in the Exploit Information.

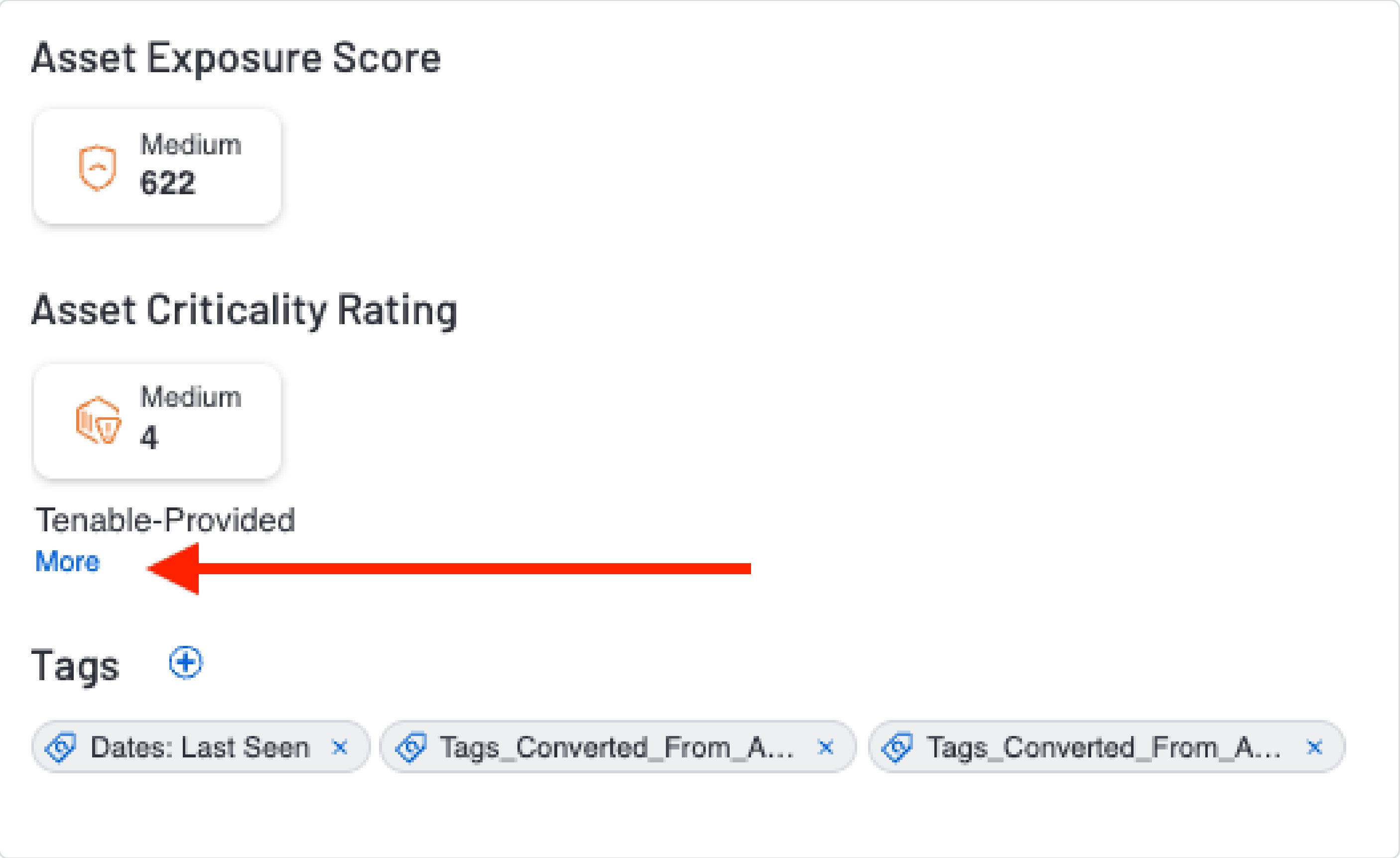
Vulnerabilities by ACR

Asset Criticality Rating (ACR) establishes the priority of each asset based on indicators of business value and criticality. ACR is based on several key metrics such as business purpose, asset type, location, connectivity, capabilities, and third-party data. ACRs range from 0 to 10. Assets with a low ACR are not considered business critical. Assets with a high ACR are considered to be the organization's most critical and carry the greater business impact if compromised. This section displays risk by ACR, Common Vulnerability Scoring System (CVSS), exploitability by Attack Vector and Framework.

The **Asset Count by ACR** widget helps track assets in the environment by grouping them based on their Asset Criticality Score (ACR). The bars are split by showing assets with an ACR score of 1-5 and then one bar per score 6 to 10. The requirements for this widget are: Tenable Vulnerability Management, Tenable Web App Scanning, and Tenable Cloud Security.



Navigate to the **Assets** page and select an asset to view the asset details and the ACR key driver information for any asset. In the lower left corner of the assets details page reference the **Asset Criticality Rating** information and click **More**.



Asset Exposure Score

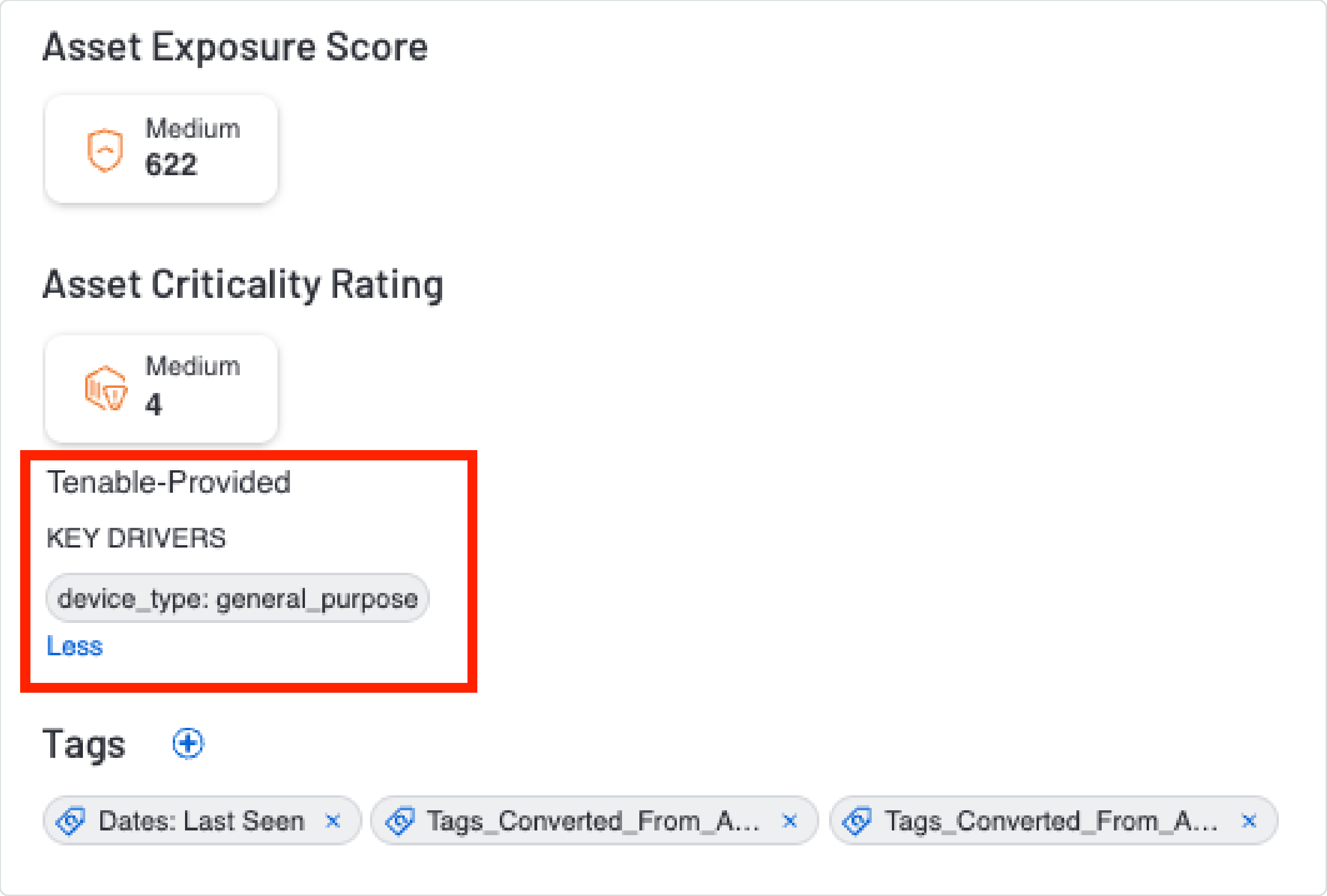
Medium
622

Asset Criticality Rating

Medium
4

Tenable-Provided

The key drivers are displayed, as shown in the following image:



Asset Exposure Score

Medium
622

Asset Criticality Rating

Medium
4

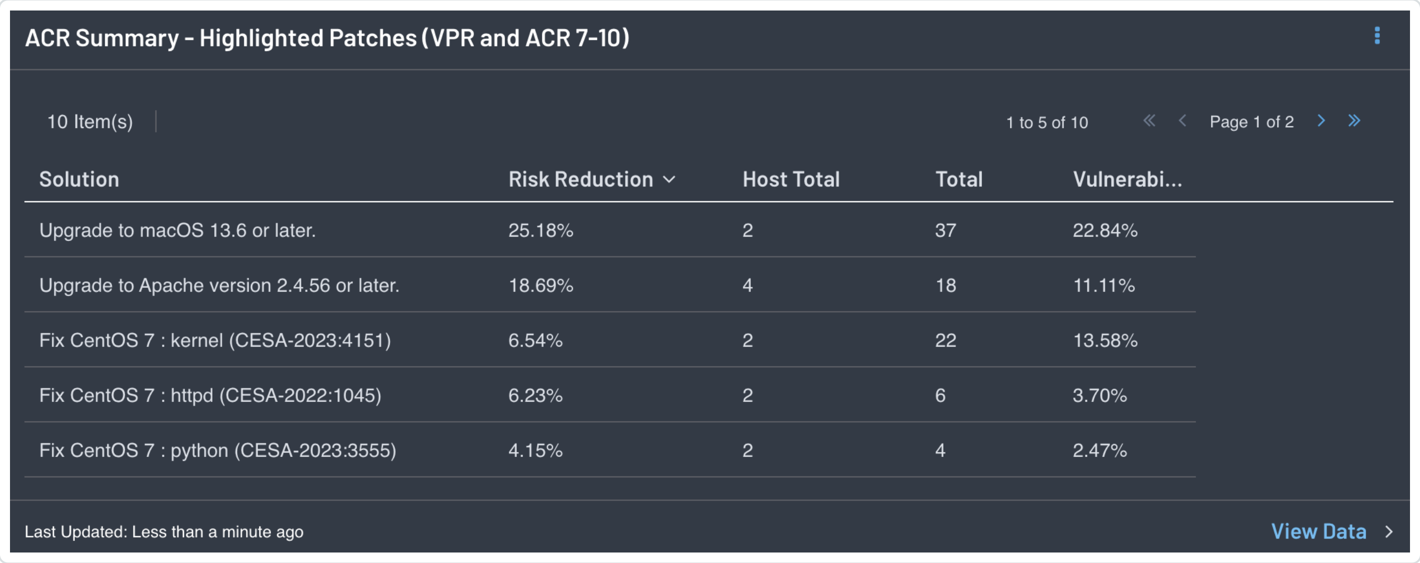
Tenable-Provided

KEY DRIVERS

device_type: general_purpose

Dates: Last Seen ×
Tags_Converted_From_A... ×
Tags_Converted_From_A... ×

Tenable Security Center has several ACR Summary components available to organizations, including the **ACR Summary - Highlighted Patches (VPR and ACR 7-10)** which provides security teams with a risk reduction plan that reduces the greatest risk when patching the highest risk vulnerabilities on the most business-critical assets. This component leverages the VPR 7-10 and ACR 7-10 filters in conjunction with the Remediation Summary tool to provide a focused view of patches that should be considered at a higher priority than other patches. The columns display recommended solutions with the greatest risk reduction at the top, as well as the associated risk reduction percentage and the host count included in the solution. Each solution can include one or more patches to be applied to one or more hosts. The Remediation Summary tool, in conjunction with the ACR filter, enables Security Teams to prioritize which vulnerabilities to remediate first for an immediate impact on the organization’s vulnerability posture



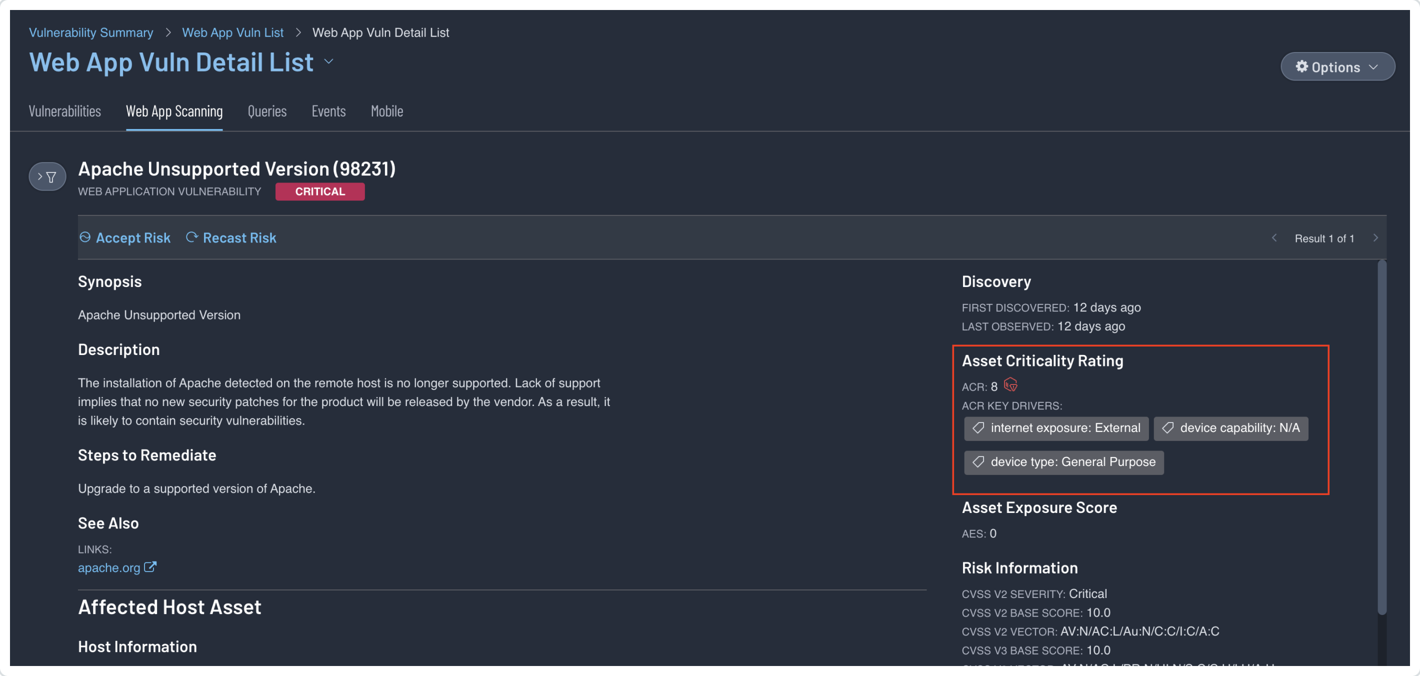
ACR Summary - Highlighted Patches (VPR and ACR 7-10)

10 Item(s) | 1 to 5 of 10 | Page 1 of 2

Solution	Risk Reduction	Host Total	Total	Vulnerabi...
Upgrade to macOS 13.6 or later.	25.18%	2	37	22.84%
Upgrade to Apache version 2.4.56 or later.	18.69%	4	18	11.11%
Fix CentOS 7 : kernel (CESA-2023:4151)	6.54%	2	22	13.58%
Fix CentOS 7 : httpd (CESA-2022:1045)	6.23%	2	6	3.70%
Fix CentOS 7 : python (CESA-2023:3555)	4.15%	2	4	2.47%

Last Updated: Less than a minute ago

Click on **View Data >** or navigate to the Analysis page and select a vulnerability to view the asset details and the ACR key driver information for any asset. In the upper right corner of the details page reference the **Asset Criticality Rating** information and **Key Drivers**.



Web App Vuln Detail List

Apache Unsupported Version (98231)

WEB APPLICATION VULNERABILITY CRITICAL

Synopsis

Apache Unsupported Version

Description

The installation of Apache detected on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Steps to Remediate

Upgrade to a supported version of Apache.

See Also

LINKS:
apache.org

Affected Host Asset

Host Information

Discovery

FIRST DISCOVERED: 12 days ago
LAST OBSERVED: 12 days ago

Asset Criticality Rating

ACR: 8

ACR KEY DRIVERS:
internet exposure: External
device capability: N/A
device type: General Purpose

Asset Exposure Score

AES: 0

Risk Information

CVSS V2 SEVERITY: Critical
CVSS V2 BASE SCORE: 10.0
CVSS V2 VECTOR: AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS V3 BASE SCORE: 10.0

Tenable assigns an ACR to each asset on the network to represent the relative criticality of the asset as an integer from 1 to 10. A higher ACR indicates higher criticality. Tenable Lumin customers have the ability to adjust the default Tenable ACR to more accurately reflect organizational risk. Refer to the Edit an ACR Manually page for more information.

Note: For customers without Tenable Lumin, the ACR is set to 0, and is reflected accordingly. Leveraging Tenable Lumin provides context of the risk per asset, making the vulnerability management program more effective.

Temporal metrics are metrics that change over time. Factors that can alter the Temporal score are: Exploit Code Maturity, Remediation Level, and Report Confidence. If a vendor has created a patch, which is widely available, the Temporal score is lower, likewise if known exploits are widely available, the score will be higher. Environmental metrics are specific to the organization, and include attributes related to the business criticality of the exposed asset, and any mitigation measures or compensating controls that are in place. Organizations can modify Environmental attributes if compensating controls are in place, thereby modifying the overall CVSS Score. The core concern is that incorrectly used Environmental score changes have a significant impact. For example, a vulnerability with a CVSS Base Score of 9.9 (Critical) and a CVSS Temporal Score of 9.9 (also Critical) has an overall score of 9.9. Combine these scores with a CVSS Environmental score of 3.2 and the Overall Score is reduced to 3.2 (Low). This is an extreme example, but illustrates what may occur if the CVSS Environmental score is modified incorrectly.

These critical pieces of information are included in ACRs, and help organizations to effectively prioritize remediation and enhance CVSS Base scores.

Remediation and Remediation Tracking

Remediation tracking is a systematic process used to monitor and manage the progress of resolving security vulnerabilities and weaknesses identified within an organization's infrastructure. Remediation tracking involves tracking the entire lifecycle of a vulnerability from discovery to resolution, ensuring that appropriate actions are taken to mitigate the identified risks. The goal of remediation tracking is to ensure vulnerabilities are addressed promptly and effectively, reducing the organization's exposure to potential threats.

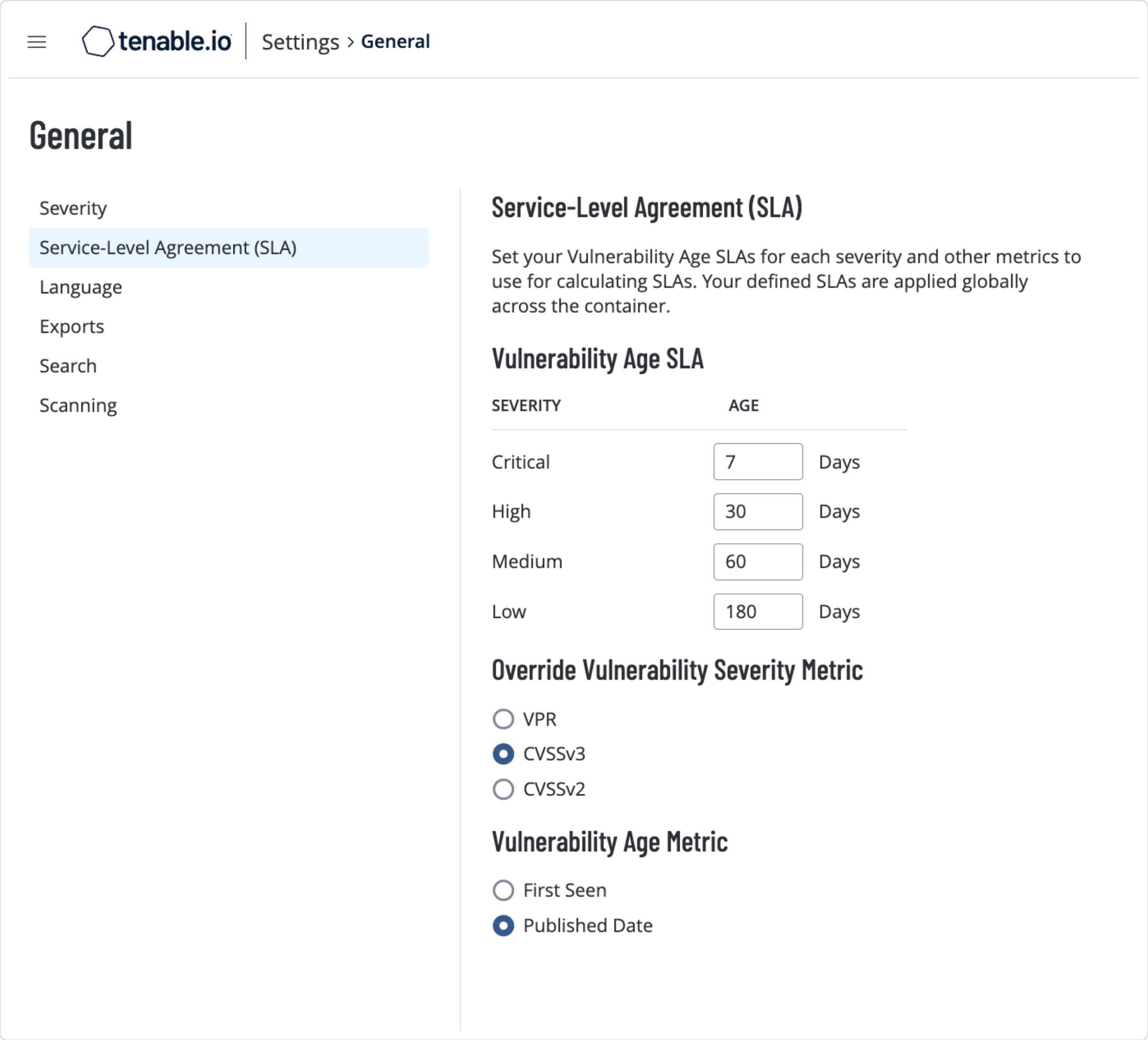
Vulnerability management Service Level Agreements (SLAs) often change from one organization to the next; however, meeting these SLAs is a common concern among organizations industry-wide. SLAs define an expected level of service by which measurements, metrics, or penalties can be established. SLA compliance is a critical component of a vulnerability management program.

There is no set timetable to resolve vulnerabilities that fits every situation. SLAs can vary from organization to organization, and even vary between business units within the organization. Tenable recommends aligning SLAs with technology or business objectives, starting with the most important assets. The Department of Homeland Security has made available 10 resource guides to help organizations implement business practices to reduce cyber risk. Volume 4: Vulnerability Management provides guidance for organizations to work with stakeholders to develop remediation timeframes that align with business goals.

As vulnerabilities are identified, remediation must be prioritized and tracked. Reviewing remediated vulnerabilities and the remediation timeframe provides valuable information to the organization on the effectiveness of the risk remediation program.

Working with SLAs

The **SLA Progress: Vulnerability Age** widget helps organizations manage Service Level Agreements (SLAs) by providing a vulnerability view organized by Vulnerability Priority Rating (VPR) Score and vulnerability age. Users can customize both the date and how the severity is calculated by selecting SLA from Tenable Vulnerability Management by navigating to the **Settings → General → Service-Level Agreement (SLA)** page.



General

Service-Level Agreement (SLA)

Set your Vulnerability Age SLAs for each severity and other metrics to use for calculating SLAs. Your defined SLAs are applied globally across the container.

Vulnerability Age SLA

SEVERITY	AGE
Critical	7 Days
High	30 Days
Medium	60 Days
Low	180 Days

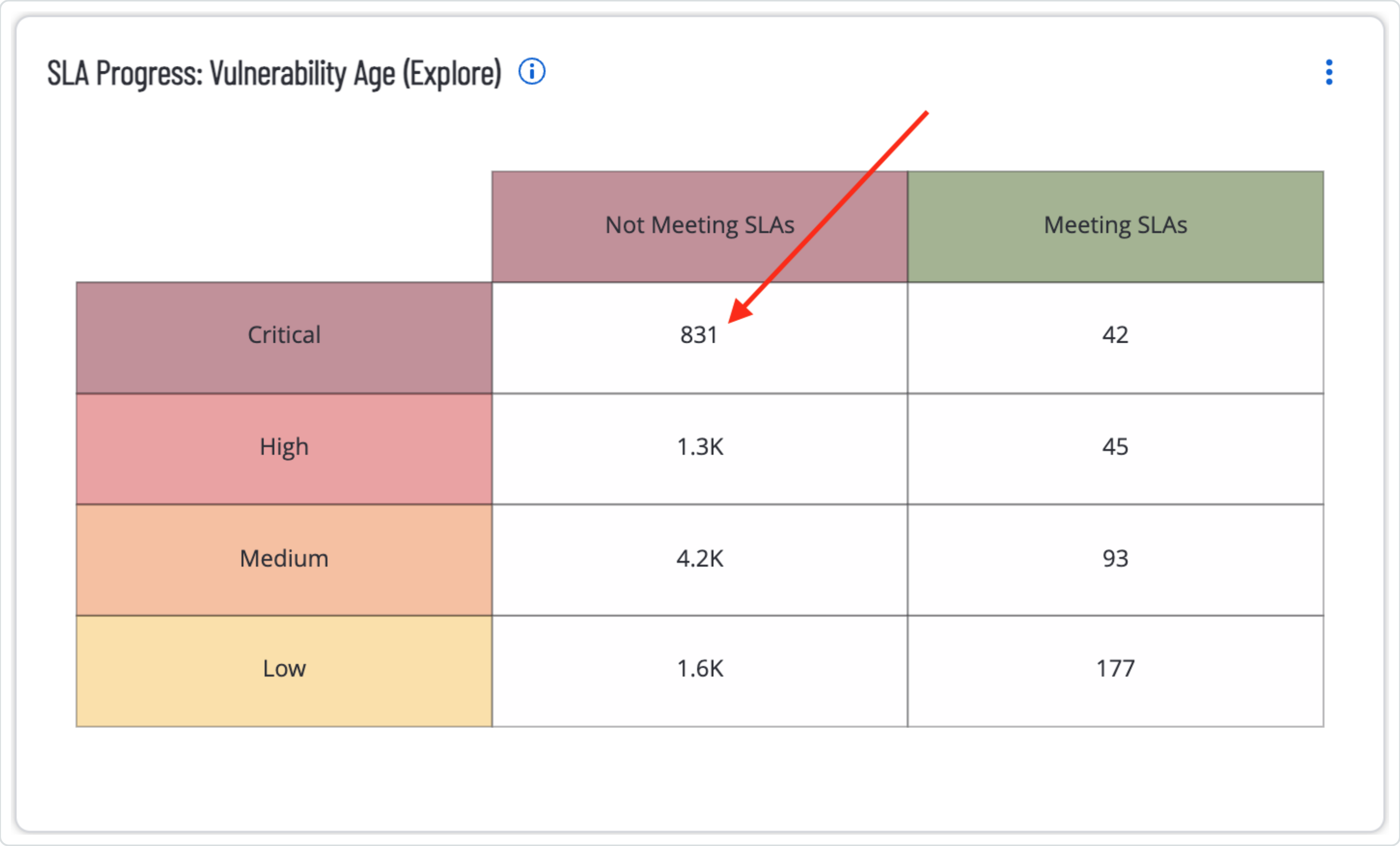
Override Vulnerability Severity Metric

○ VPR
● CVSSv3
○ CVSSv2

Vulnerability Age Metric

○ First Seen
● Published Date

The vulnerabilities that do not meet SLAs are calculated using a date filter for within the last X days. The vulnerabilities that meet SLAs use a date filter for older than X days. When default SLA settings are used, the Critical row displays vulnerabilities with a VPR score greater than 9.0. The High row displays those with VPR between 7.0-8.9, the Medium row displays VPR between 4.0-6.9, and the Low row displays VPR between 0-3.9.

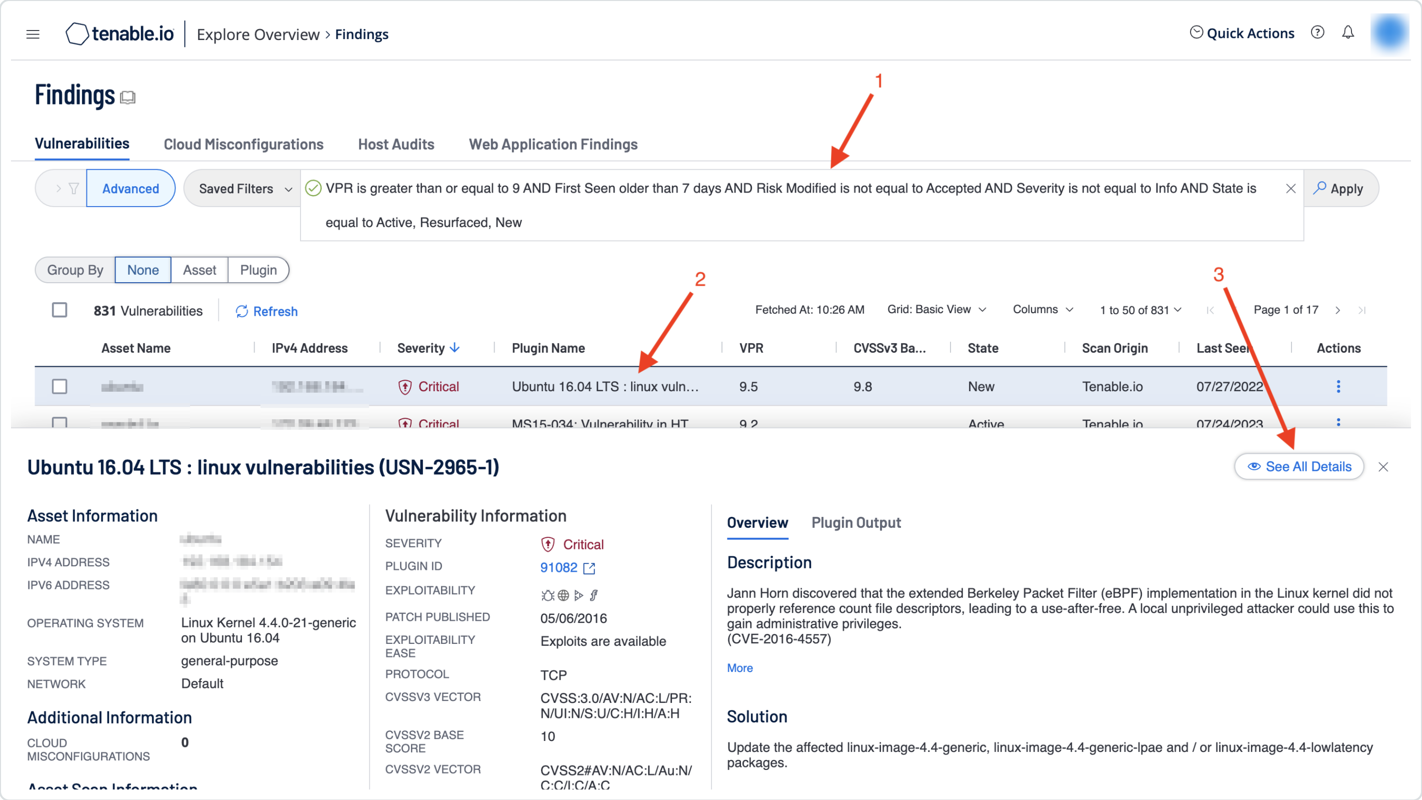


SLA Progress: Vulnerability Age (Explore)

	Not Meeting SLAs	Meeting SLAs
Critical	831	42
High	1.3K	45
Medium	4.2K	93
Low	1.6K	177

Drilling Down

Clicking a cell in the widget shown above provides greater details about the vulnerabilities in the category, as shown in the following image:



VPR is greater than or equal to 9 AND First Seen older than 7 days AND Risk Modified is not equal to Accepted AND Severity is not equal to Info AND State is equal to Active, Resurfaced, New

831 Vulnerabilities

	Asset Name	IPv4 Address	Severity	Plugin Name	VPR	CVSSv3 Ba...	State	Scan Origin	Last Seen	Actions
□	[redacted]	[redacted]	Critical	Ubuntu 16.04 LTS : linux vuln...	9.5	9.8	New	Tenable.io	07/27/2022	⋮
□	[redacted]	[redacted]	Critical	MS15-034: Vulnerability in HT	9.2		Active	Tenable.io	07/24/2023	⋮

Ubuntu 16.04 LTS : linux vulnerabilities (USN-2965-1)

Asset Information

NAME	[redacted]
IPV4 ADDRESS	[redacted]
IPV6 ADDRESS	[redacted]
OPERATING SYSTEM	Linux Kernel 4.4.0-21-generic on Ubuntu 16.04
SYSTEM TYPE	general-purpose
NETWORK	Default

Additional Information

CLOUD MISCONFIGURATIONS	0

Asset Scan Information

Vulnerability Information

SEVERITY	Critical
PLUGIN ID	91082
EXPLOITABILITY	
PATCH PUBLISHED	05/06/2016
EXPLOITABILITY EASE	Exploits are available
PROTOCOL	TCP
CVSSV3 VECTOR	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSSV2 BASE SCORE	10
CVSSV2 VECTOR	CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

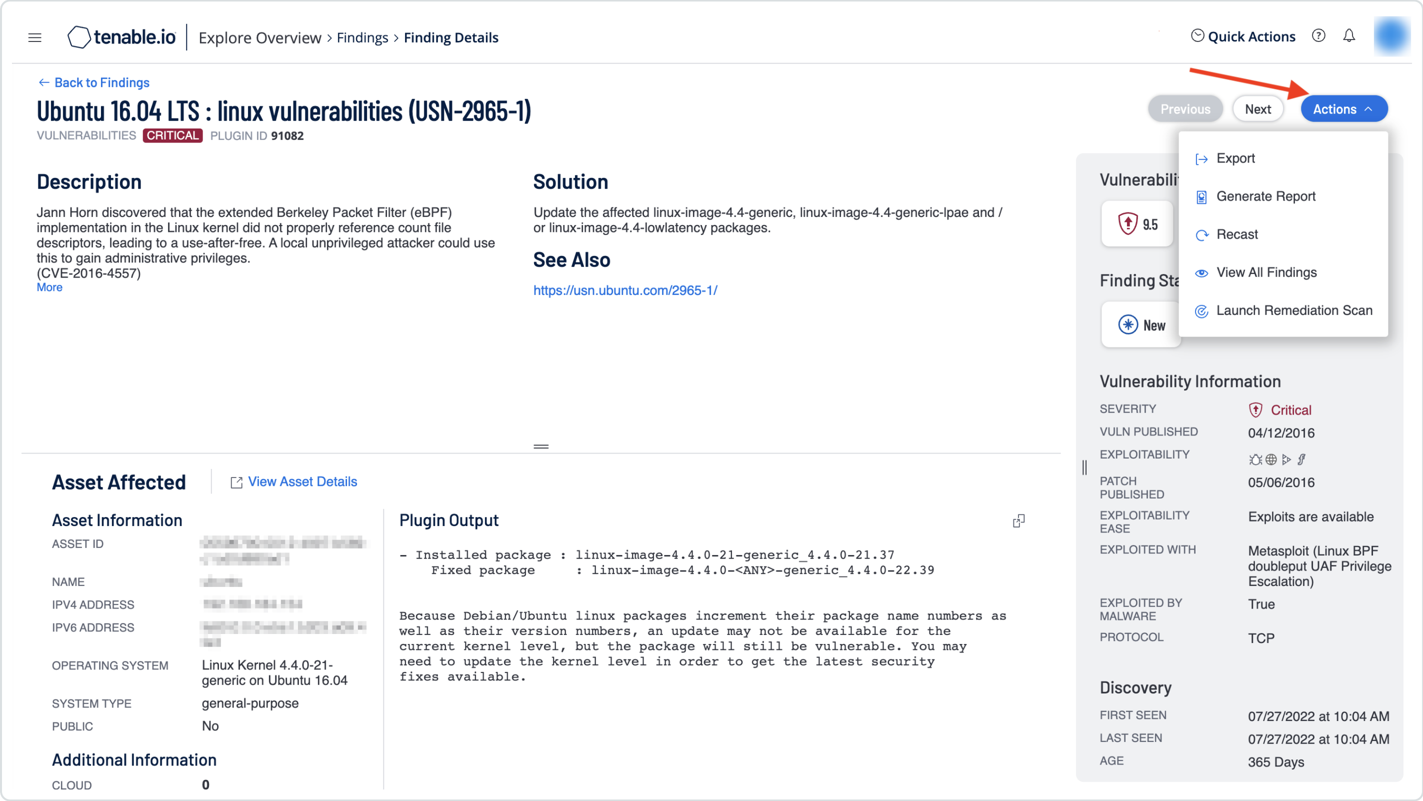
Description

Jann Horn discovered that the extended Berkeley Packet Filter (eBPF) implementation in the Linux kernel did not properly reference count file descriptors, leading to a use-after-free. A local unprivileged attacker could use this to gain administrative privileges.
(CVE-2016-4557)

Solution

Update the affected linux-image-4.4-generic, linux-image-4.4-generic-lpae and / or linux-image-4.4-lowlatency packages.

The **Conditions** field (**1**) displays the filter used for this search. Clicking on the **Plugin** name (**2**) provides an overview of the particular plugin, in the example shown above, the plugin was **Ubuntu 16.04 LTS: linux vulnerabilities (USN-2965-1)**. Clicking the **See all Details** button (**3**) provides even greater details about the affected asset and additional vulnerability information, as shown in the following image:



Ubuntu 16.04 LTS : linux vulnerabilities (USN-2965-1)

VULNERABILITIES CRITICAL PLUGIN ID 91082

Description

Jann Horn discovered that the extended Berkeley Packet Filter (eBPF) implementation in the Linux kernel did not properly reference count file descriptors, leading to a use-after-free. A local unprivileged attacker could use this to gain administrative privileges.
(CVE-2016-4557)
More

Solution

Update the affected linux-image-4.4-generic, linux-image-4.4-generic-lpae and / or linux-image-4.4-lowlatency packages.

See Also

https://usn.ubuntu.com/2965-1/

Asset Affected

Asset Information

ASSET ID	[redacted]
NAME	[redacted]
IPV4 ADDRESS	[redacted]
IPV6 ADDRESS	[redacted]
OPERATING SYSTEM	Linux Kernel 4.4.0-21-generic on Ubuntu 16.04
SYSTEM TYPE	general-purpose
PUBLIC	No

Additional Information

CLOUD	0

Plugin Output

```
- Installed package : linux-image-4.4.0-21-generic_4.4.0-21.37
    Fixed package     : linux-image-4.4.0-<ANY>-generic_4.4.0-22.39


Because Debian/Ubuntu linux packages increment their package name numbers as
well as their version numbers, an update may not be available for the
current kernel level, but the package will still be vulnerable. You may
need to update the kernel level in order to get the latest security
fixes available.
```

Vulnerability Information

SEVERITY	Critical
VULN PUBLISHED	04/12/2016
EXPLOITABILITY	
PATCH PUBLISHED	05/06/2016
EXPLOITABILITY EASE	Exploits are available
EXPLOITED WITH	Metasploit (Linux BPF doublepout UAF Privilege Escalation)
EXPLOITED BY MALWARE	True
PROTOCOL	TCP

Discovery

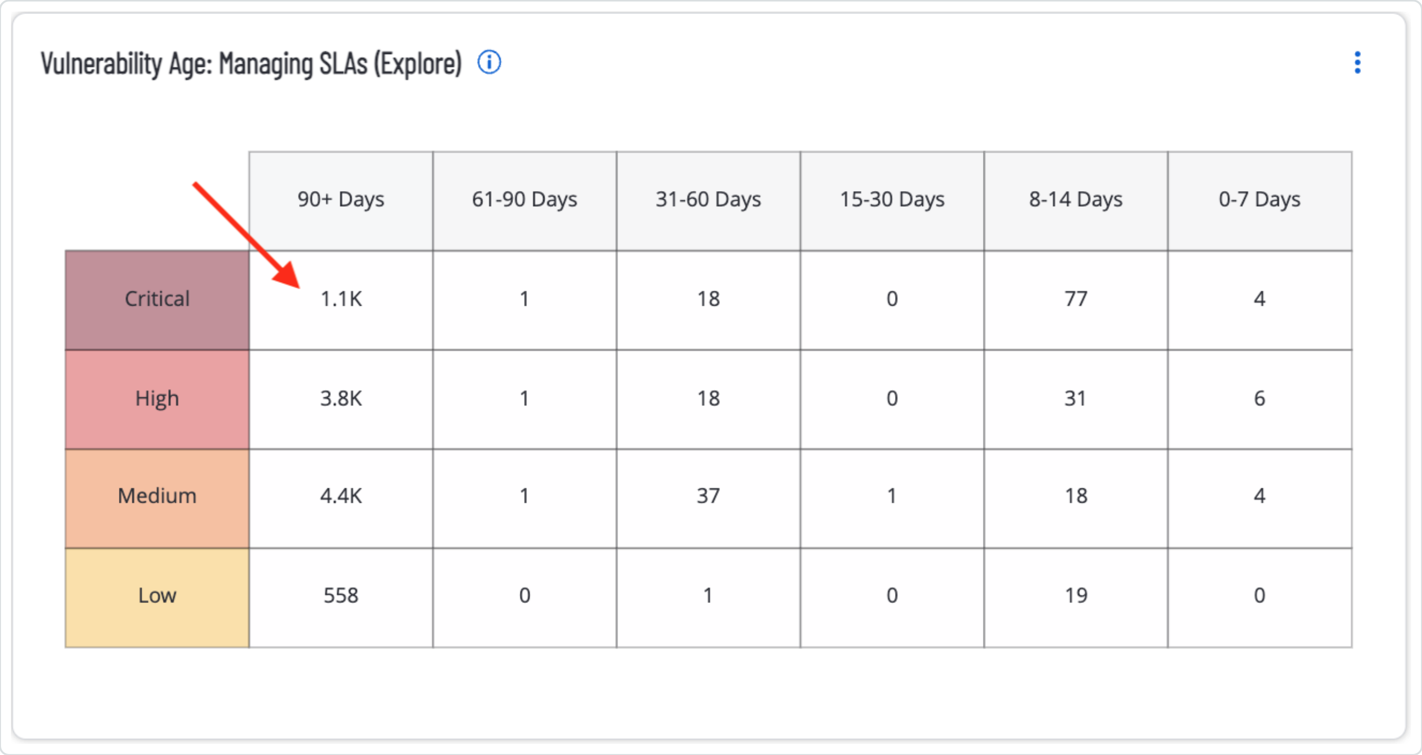
FIRST SEEN	07/27/2022 at 10:04 AM
LAST SEEN	07/27/2022 at 10:04 AM
AGE	365 Days

From this view, additional actions can be taken regarding the affected asset.

Outstanding Remediations

The time between when a vulnerability is discovered and when the vulnerability is typically exploited, or 'time to exploit' is rapidly decreasing. The CISA INSIGHTS report titled Remediate Vulnerabilities for Internet-Accessible Systems notes adversaries, on average, are able to exploit a vulnerability within 15 days. This is down from a previous average of over 30 days the previous year. This means that patching must be a priority for organizations to reduce threats as unpatched vulnerabilities over 15 days old begin to present a significant risk.

The **Vulnerability Age: Managing SLAs** widget provides a view of vulnerabilities based on severity and age. The columns display counts of vulnerabilities, which have been published within the specified time period, and are present in the organization. The rows display the severity level of the vulnerability.

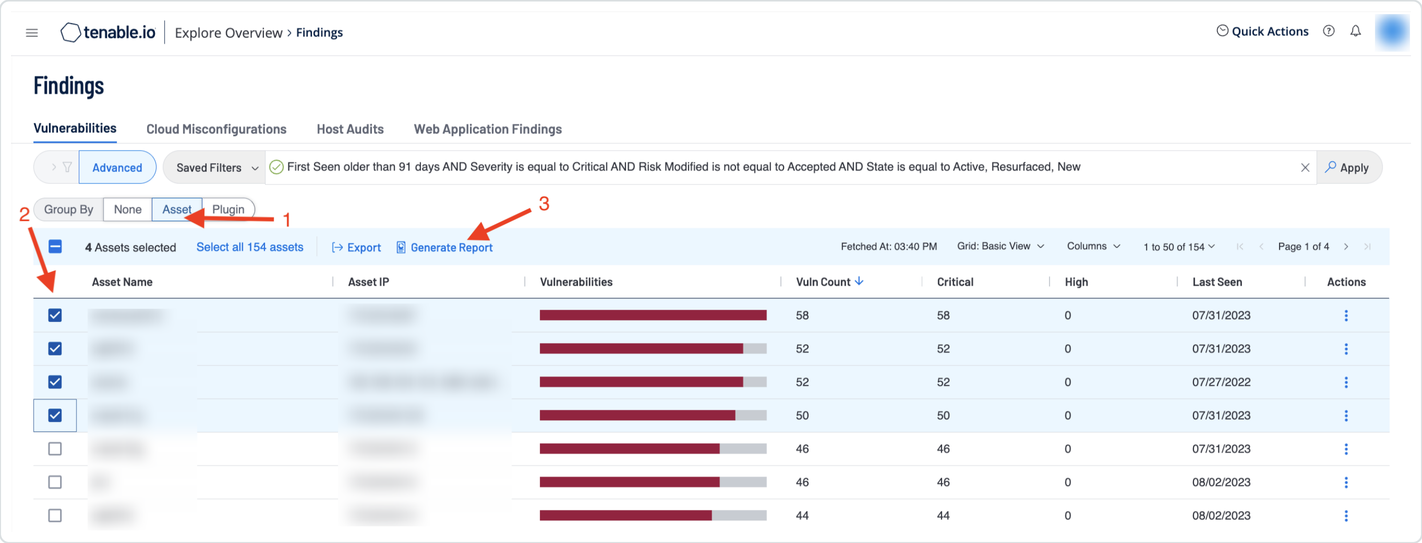


Vulnerability Age: Managing SLAs (Explore)

	90+ Days	61-90 Days	31-60 Days	15-30 Days	8-14 Days	0-7 Days
Critical	1.1K	1	18	0	77	4
High	3.8K	1	18	0	31	6
Medium	4.4K	1	37	1	18	4
Low	558	0	1	0	19	0

Drilling Down in Tenable Vulnerability Management

Security analysts can easily generate a report on the assets posing the greatest risk for outstanding remediations by drilling down into the details from this widget. Click on the cell with the most Critical vulnerabilities, which have been outstanding for over 90 days, and select **Asset** (**1**). In the following example, select the desired assets (**2**) and then select **Generate Report** (**3**).

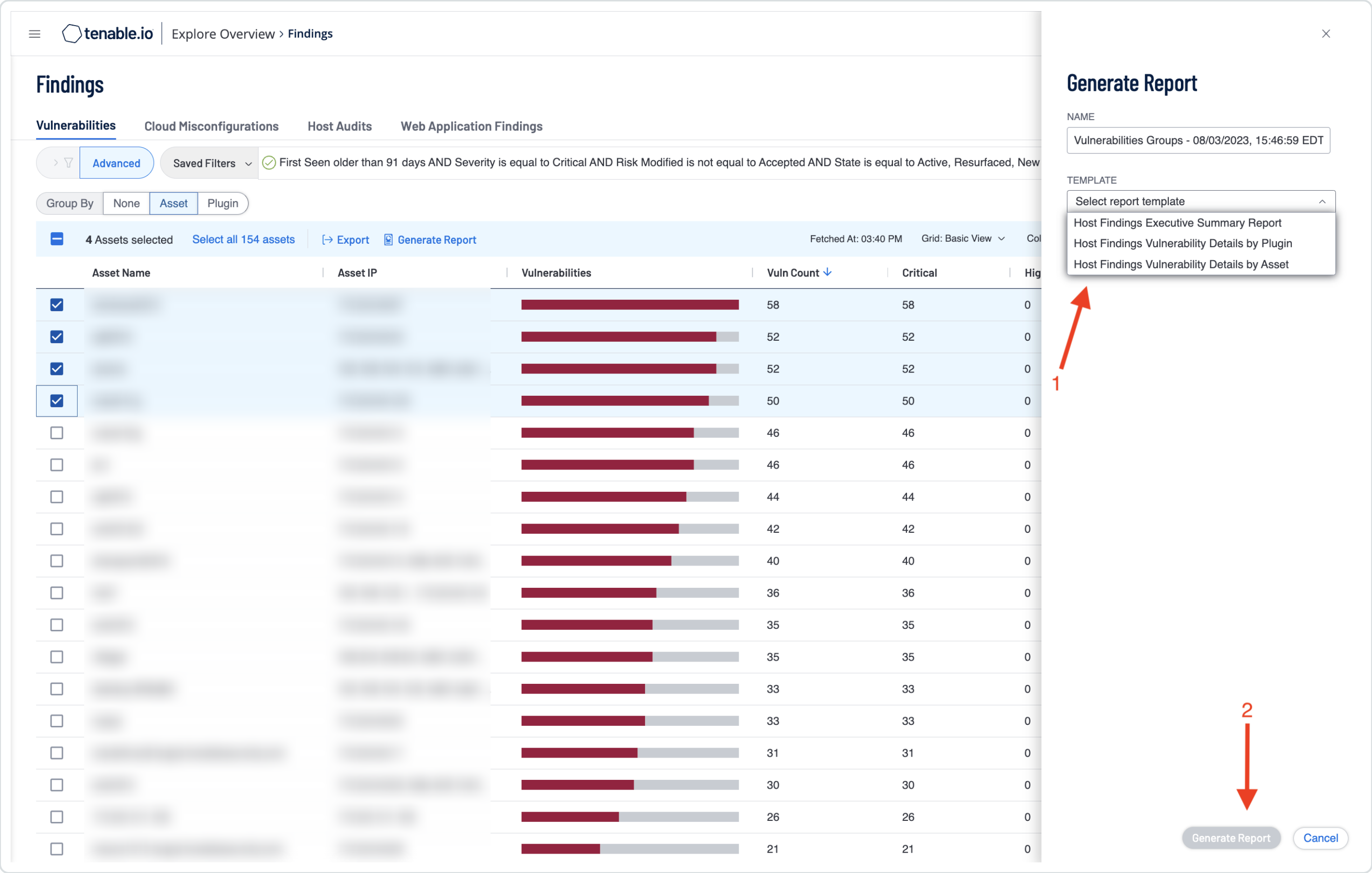


First Seen older than 91 days AND Severity is equal to Critical AND Risk Modified is not equal to Accepted AND State is equal to Active, Resurfaced, New

4 Assets selected | Select all 154 assets | Fetched At: 03:40 PM | 1 to 50 of 154

	Asset Name	Asset IP	Vulnerabilities	Vuln Count ↓	Critical	High	Last Seen	Actions
☑	[redacted]	[redacted]		58	58	0	07/31/2023	⋮
☑	[redacted]	[redacted]		52	52	0	07/31/2023	⋮
☑	[redacted]	[redacted]		52	52	0	07/27/2022	⋮
☑	[redacted]	[redacted]		50	50	0	07/31/2023	⋮
☐	[redacted]	[redacted]		46	46	0	07/31/2023	⋮
☐	[redacted]	[redacted]		46	46	0	08/02/2023	⋮
☐	[redacted]	[redacted]		44	44	0	08/02/2023	⋮

The **Generate Report** window is displayed, where the type of report, such as "**Host Findings Vulnerability Details by Asset**" can be selected (**1**), followed by clicking on the **Generate Report** button (**2**).



tenable.io | Explore Overview › Findings

Findings

Vulnerabilities | Cloud Misconfigurations | Host Audits | Web Application Findings

Advanced | Saved Filters | First Seen older than 91 days AND Severity is equal to Critical AND Risk Modified is not equal to Accepted AND State is equal to Active, Resurfaced, New

Group By: None | Asset | Plugin

4 Assets selected | Select all 154 assets | Export | Generate Report | Fetched At: 03:40 PM | Grid: Basic View

	Asset Name	Asset IP	Vulnerabilities	Vuln Count	Critical	Hig
☑	[redacted]	[redacted]		58	58	0
☑	[redacted]	[redacted]		52	52	0
☑	[redacted]	[redacted]		52	52	0
☑	[redacted]	[redacted]		50	50	0
□	[redacted]	[redacted]		46	46	0
□	[redacted]	[redacted]		46	46	0
□	[redacted]	[redacted]		44	44	0
□	[redacted]	[redacted]		42	42	0
□	[redacted]	[redacted]		40	40	0
□	[redacted]	[redacted]		36	36	0
□	[redacted]	[redacted]		35	35	0
□	[redacted]	[redacted]		35	35	0
□	[redacted]	[redacted]		33	33	0
□	[redacted]	[redacted]		33	33	0
□	[redacted]	[redacted]		31	31	0
□	[redacted]	[redacted]		30	30	0
□	[redacted]	[redacted]		26	26	0
□	[redacted]	[redacted]		21	21	0

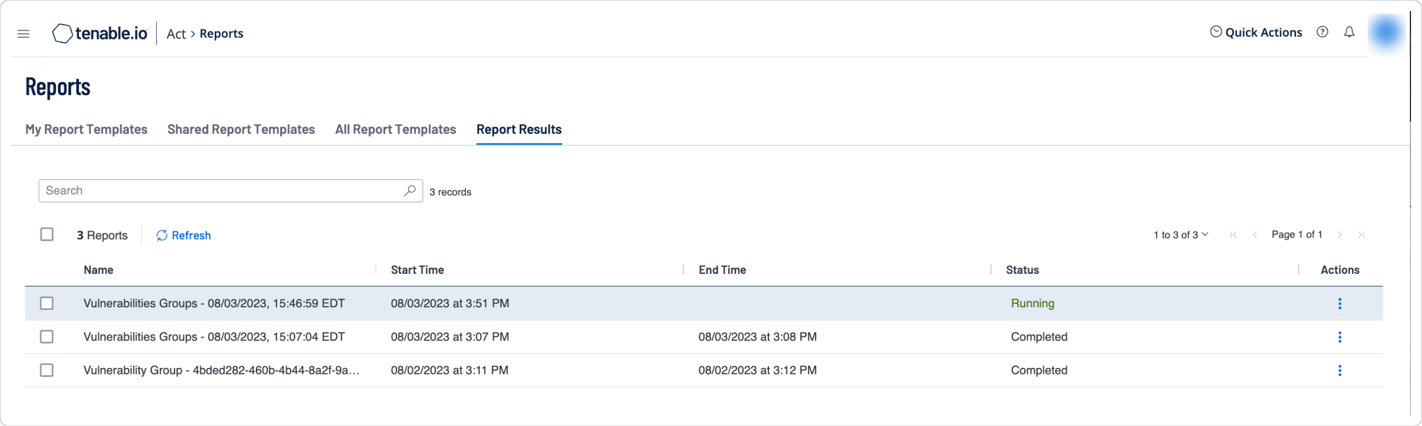
Generate Report

NAME: Vulnerabilities Groups - 08/03/2023, 15:46:59 EDT

TEMPLATE: Select report template

- Host Findings Executive Summary Report
- Host Findings Vulnerability Details by Plugin
- Host Findings Vulnerability Details by Asset

The **Report Results** page displays the running report, as shown:



tenable.io | Act › Reports | Quick Actions

Reports

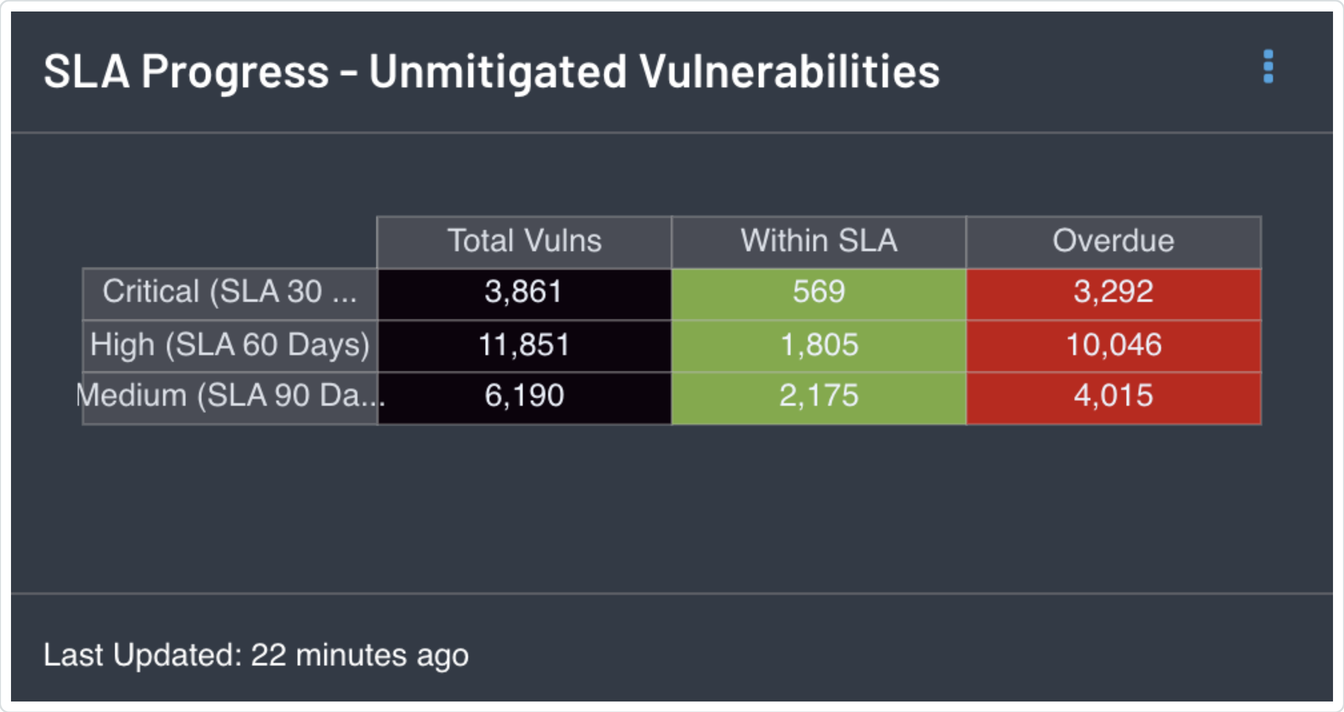
My Report Templates | Shared Report Templates | All Report Templates | Report Results

Search | 3 records

□ 3 Reports | Refresh | 1 to 3 of 3 | Page 1 of 1

	Name	Start Time	End Time	Status	Actions
□	Vulnerabilities Groups - 08/03/2023, 15:46:59 EDT	08/03/2023 at 3:51 PM		Running	⋮
□	Vulnerabilities Groups - 08/03/2023, 15:07:04 EDT	08/03/2023 at 3:07 PM	08/03/2023 at 3:08 PM	Completed	⋮
□	Vulnerability Group - 4bded282-460b-4b44-8a2f-9a...	08/02/2023 at 3:11 PM	08/02/2023 at 3:12 PM	Completed	⋮

Tenable Security Center does not have a configuration option to define organization specific SLA time-frames. In lieu of that, the **SLA Progress - Unmitigated Vulnerabilities** component provides a summary of vulnerabilities based on the CVSS score and the SLA of 30, 60, 90 days. The best practice is to mitigate critical vulnerabilities in under 30 days, ~30 days for high, 60 for medium, and 90 for low.



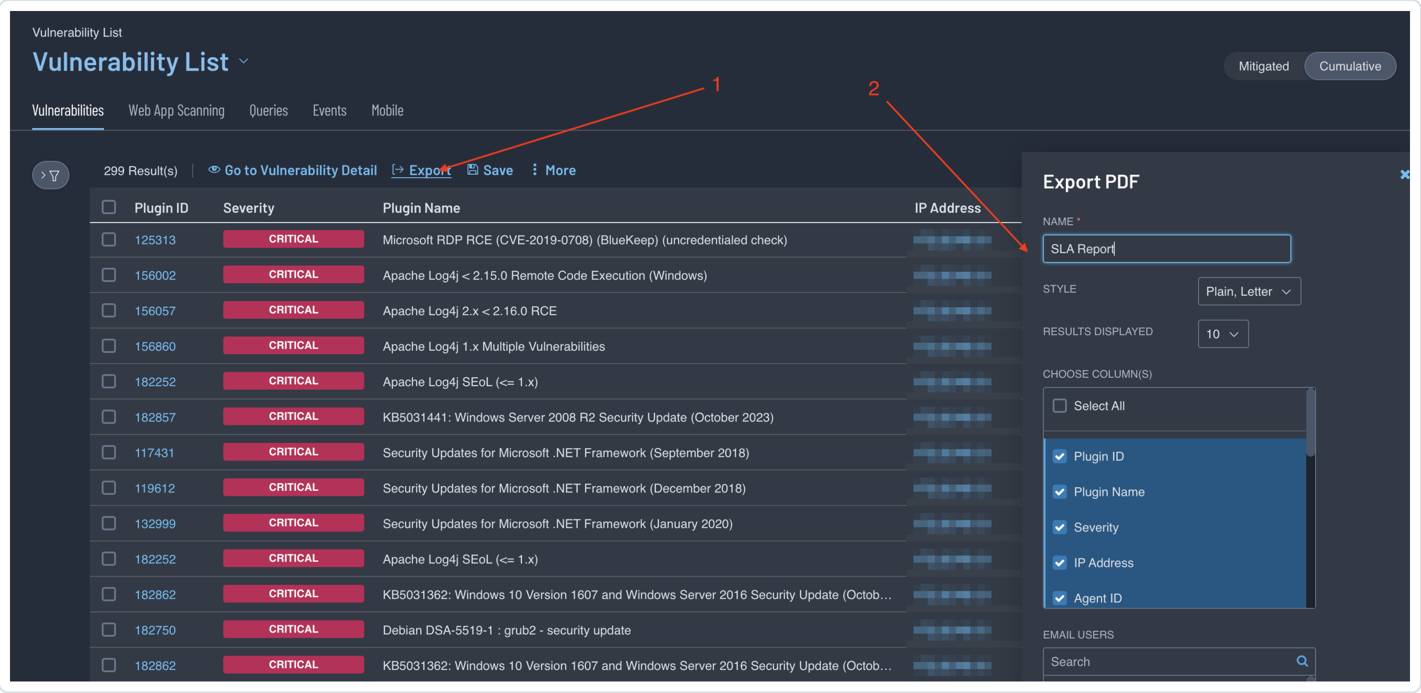
SLA Progress - Unmitigated Vulnerabilities

	Total Vulns	Within SLA	Overdue
Critical (SLA 30 ...	3,861	569	3,292
High (SLA 60 Days)	11,851	1,805	10,046
Medium (SLA 90 Da...	6,190	2,175	4,015

Last Updated: 22 minutes ago

Drilling Down in Tenable Security Center

Security analysts can easily generate a report on the assets overdue, or within SLAs by drilling down into the details from this component . Click on the appropriate cell in the component, and from the Vulnerability Analysis page click on Export (1), and select CSV or PDF (in this example PDF was chosen). From the box that open on the right side of the page (2), enter a name for check the appropriate information, finally scroll to the bottom of the box and click submit.



Vulnerability List

Vulnerability List

Mitigated | Cumulative

Vulnerabilities | Web App Scanning | Queries | Events | Mobile

299 Result(s) | Go to Vulnerability Detail | Export | Save | More

Plugin ID	Severity	Plugin Name	IP Address
125313	CRITICAL	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)	[redacted]
156002	CRITICAL	Apache Log4j < 2.15.0 Remote Code Execution (Windows)	[redacted]
156057	CRITICAL	Apache Log4j 2.x < 2.16.0 RCE	[redacted]
156860	CRITICAL	Apache Log4j 1.x Multiple Vulnerabilities	[redacted]
182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]
182857	CRITICAL	KB5031441: Windows Server 2008 R2 Security Update (October 2023)	[redacted]
117431	CRITICAL	Security Updates for Microsoft .NET Framework (September 2018)	[redacted]
119612	CRITICAL	Security Updates for Microsoft .NET Framework (December 2018)	[redacted]
132999	CRITICAL	Security Updates for Microsoft .NET Framework (January 2020)	[redacted]
182252	CRITICAL	Apache Log4j SEoL (<= 1.x)	[redacted]
182862	CRITICAL	KB5031362: Windows 10 Version 1607 and Windows Server 2016 Security Update (Octob…	[redacted]
182750	CRITICAL	Debian DSA-5519-1 : grub2 - security update	[redacted]
182862	CRITICAL	KB5031362: Windows 10 Version 1607 and Windows Server 2016 Security Update (Octob…	[redacted]

Export PDF

NAME *: SLA Report

STYLE: Plain, Letter

RESULTS DISPLAYED: 10

CHOOSE COLUMN(S)

□ Select All

☑ Plugin ID

☑ Plugin Name

☑ Severity

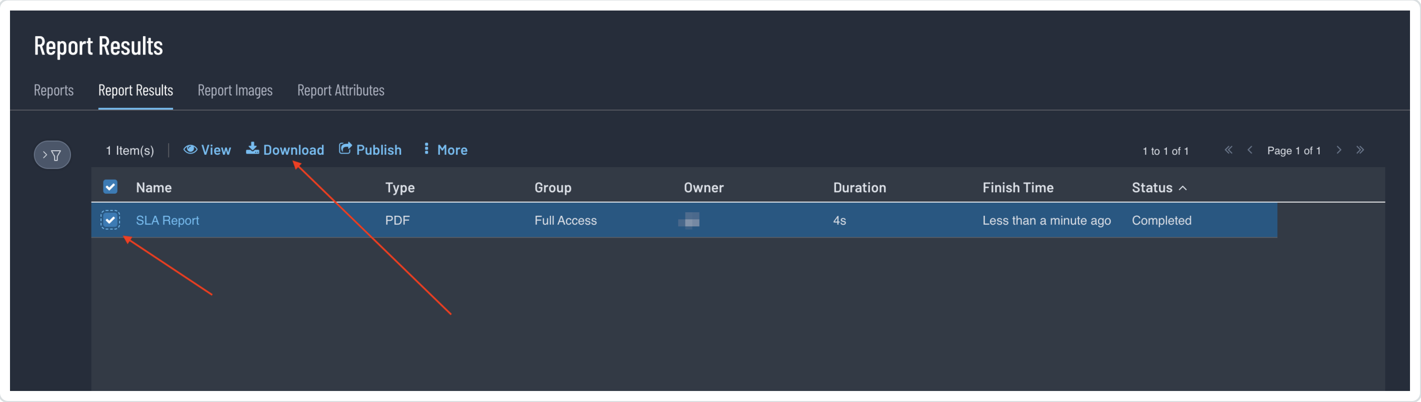
☑ IP Address

☑ Agent ID

EMAIL USERS

Search

A report will generate and will be available on the Report page. Check the box next to the report and then download the report to view the details.



Report Results

Reports | Report Results | Report Images | Report Attributes

1 Item(s) | View | Download | Publish | More

1 to 1 of 1 | Page 1 of 1

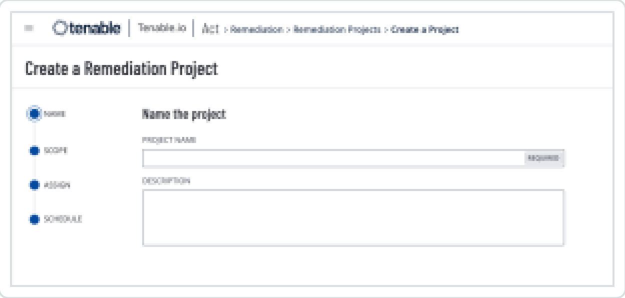
	Name	Type	Group	Owner	Duration	Finish Time	Status
☑	SLA Report	PDF	Full Access	[redacted]	4s	Less than a minute ago	Completed

Remediation Summary

Unpatched assets expose organizations to vulnerabilities that can be exploited. When new assets are added to the network and scanned for the first time, any related vulnerabilities for which a patch has been available but not applied are displayed. Ideally, organizations with an effective vulnerability management process patches vulnerabilities during the initial build process.

Assets with the largest number of missing patches typically represent a higher level of remediation effort and may be the most time-consuming to address. Vulnerability severity, exploitability, and time since a patch was made available are displayed as the key points of vulnerability management. Organizations with an effective vulnerability management program will typically patch within 90 days of the date the patch is made available, and usually has lower counts in the last two rows of these matrices. These organizations will most likely only have data presented in the first row (under 30 days), especially for the highest severity vulnerabilities.

Assets that are exploitable or have a higher severity rating represent a fast lane for attackers. Prioritizing remediation of these vulnerabilities is an effective strategy to reduce risk. Tenable has provided a method to create a Remediation Project so findings can be prioritized, the scope of work can be defined, projects can be assigned, and progress can be tracked. Remediation projects can be set to be completed at a fixed date, or within a specified timeframe.


tenable
Tenable.io
Act > Remediation > Remediation Projects > Create a Project
Create a Remediation Project
NAME
SCOPE
ASSIGN
SCHEDULE
Name the project
PROJECT NAME
REQUIRED
DESCRIPTION

More information on the creation, viewing, editing, closing, or suspending of remediation projects can be found on the Remediation Projects page of the Tenable documentation. Remediation projects, which are created within Tenable Vulnerability Management, can also be exported as a .csv for use outside of Tenable Vulnerability Management.

Learn More

Tenable Resources

- Tenable Plugins page
- Tenable OWASP Report
- Tenable OWASP Dashboard
- What is VPR and How is it Different From CVSS
- Getting Started with Tenable Identity Exposure
- Tenable Cyber Exposure Study: Identity and Access Management
- Getting Started with Active Directory
- Tenable Indicators of Attack
- Tenable Indicators of Exposure
- Tenable Cyber Exposure Study: Establishing a Software Inventory
- Audits Search page
- Unsupported Software Dashboard post
- Asset Criticality Rating
- Edit an ACR Manually
- Remediation Projects documentation

Compliance References

- CIS Control 16: Application Software Security
- CIS Control 16: Application Software Security
- Common Vulnerability Scoring System
- National Vulnerability Database
- NIST Special Publication 800-53 Rev 5
- NIST Mapping to HIPAA Security Rule

- ISO/IEC 27001 Standard
- OSWASP Top 10:2021
- General Data Protection Regulation (GDPR - EU)
- Data Protection Act (UK)
- Payment Card Industry Data Security Standard (PCI DSS)