Tenable Cyber Exposure Study – Application Software Security

Last Revised: July 17, 2025

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.

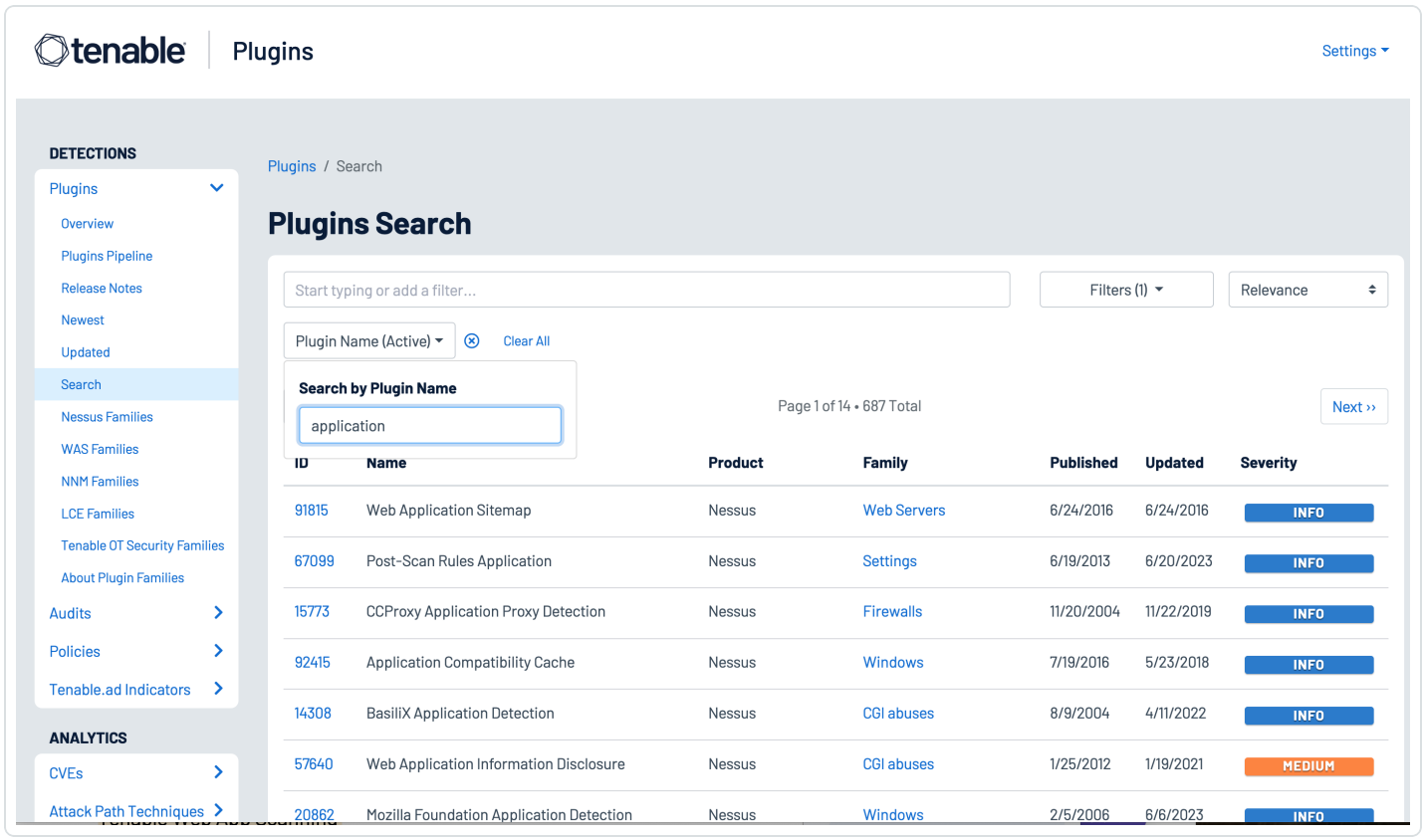
This guide provides a detailed approach to application security and includes information to address key focus areas such as:

- **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:



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.

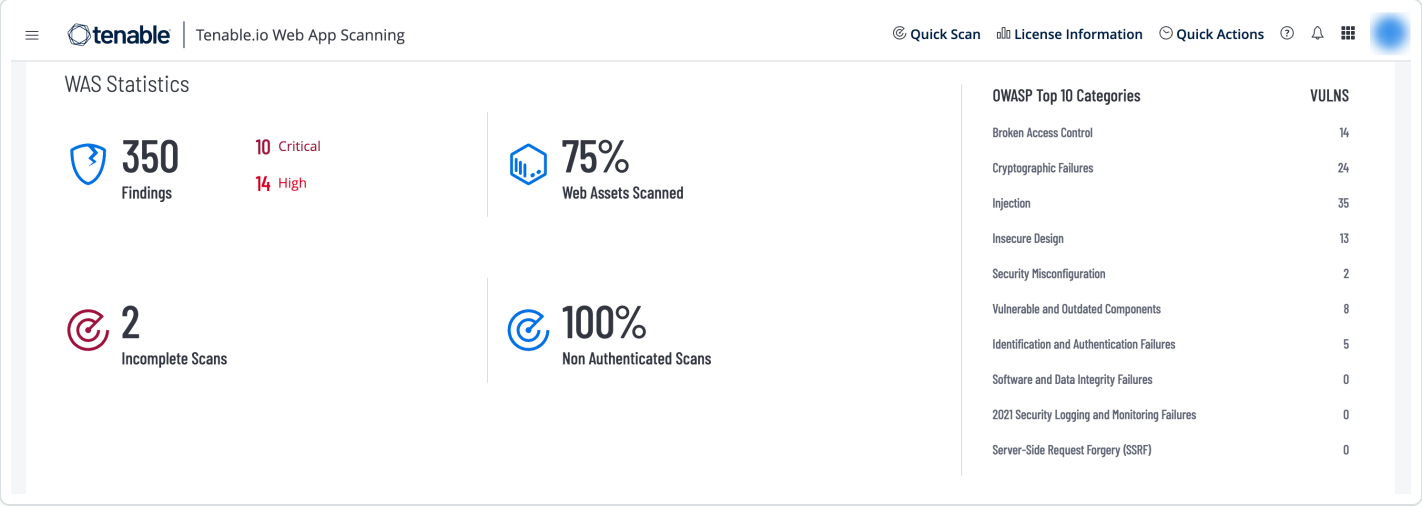
Web application scanning is of critical importance because users typically access these applications from a browser over the internet. Web applications exist on remote servers or in cloud environments, and data is transmitted over public networks. Web application security is a critical aspect to ensure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

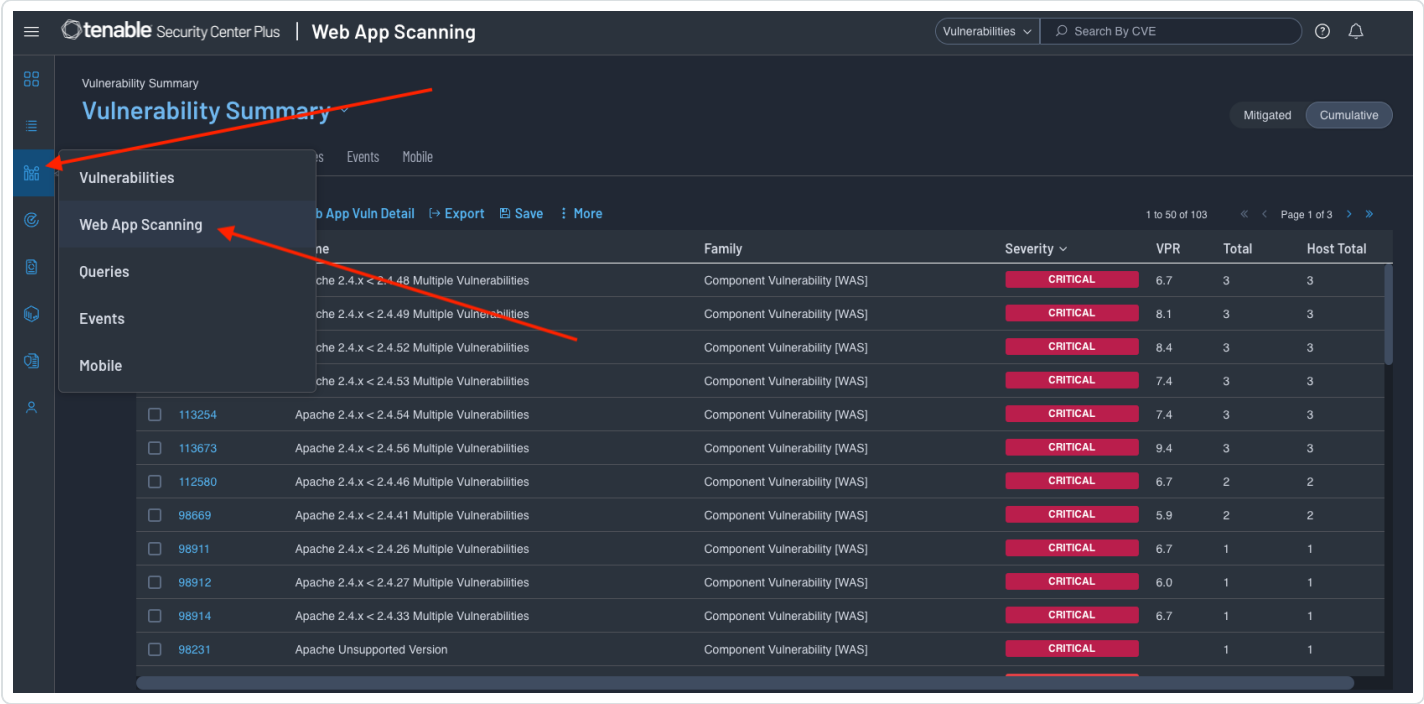
Tenable Web App Scanning analyzes web applications and provides deep-dive data on OWASP top 10 vulnerabilities, component vulnerabilities, injections, and in-depth informational details to help organizations identify security concerns in their web applications. The Tenable Web App Scanning landing page 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.



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

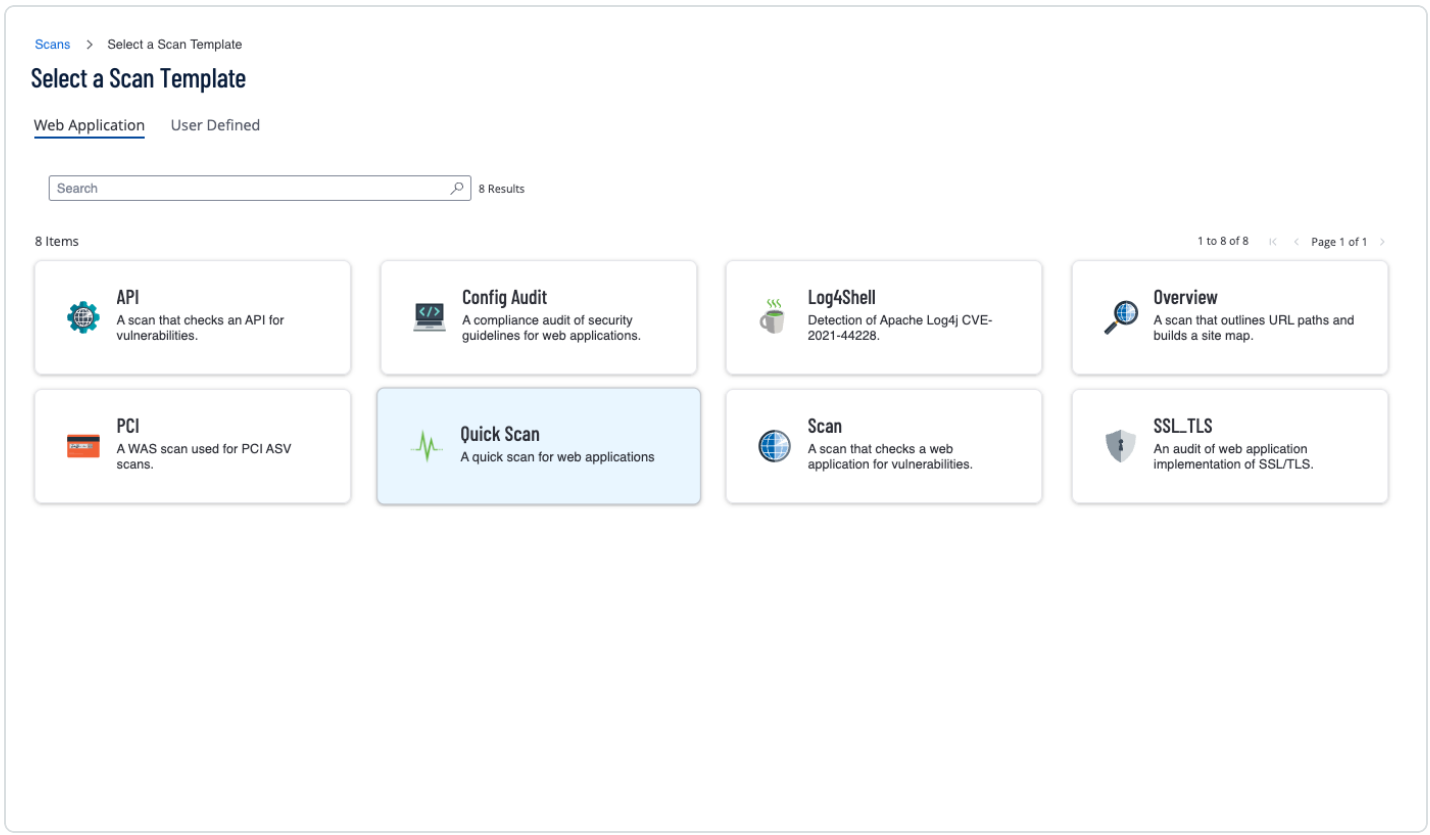
and strategize remediation based on the immediate risk a vulnerability poses. Updated scan export and new scan import capabilities enables users to import exported scans and see debugging information in web application scan exports to assist with troubleshooting.

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.



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.



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.

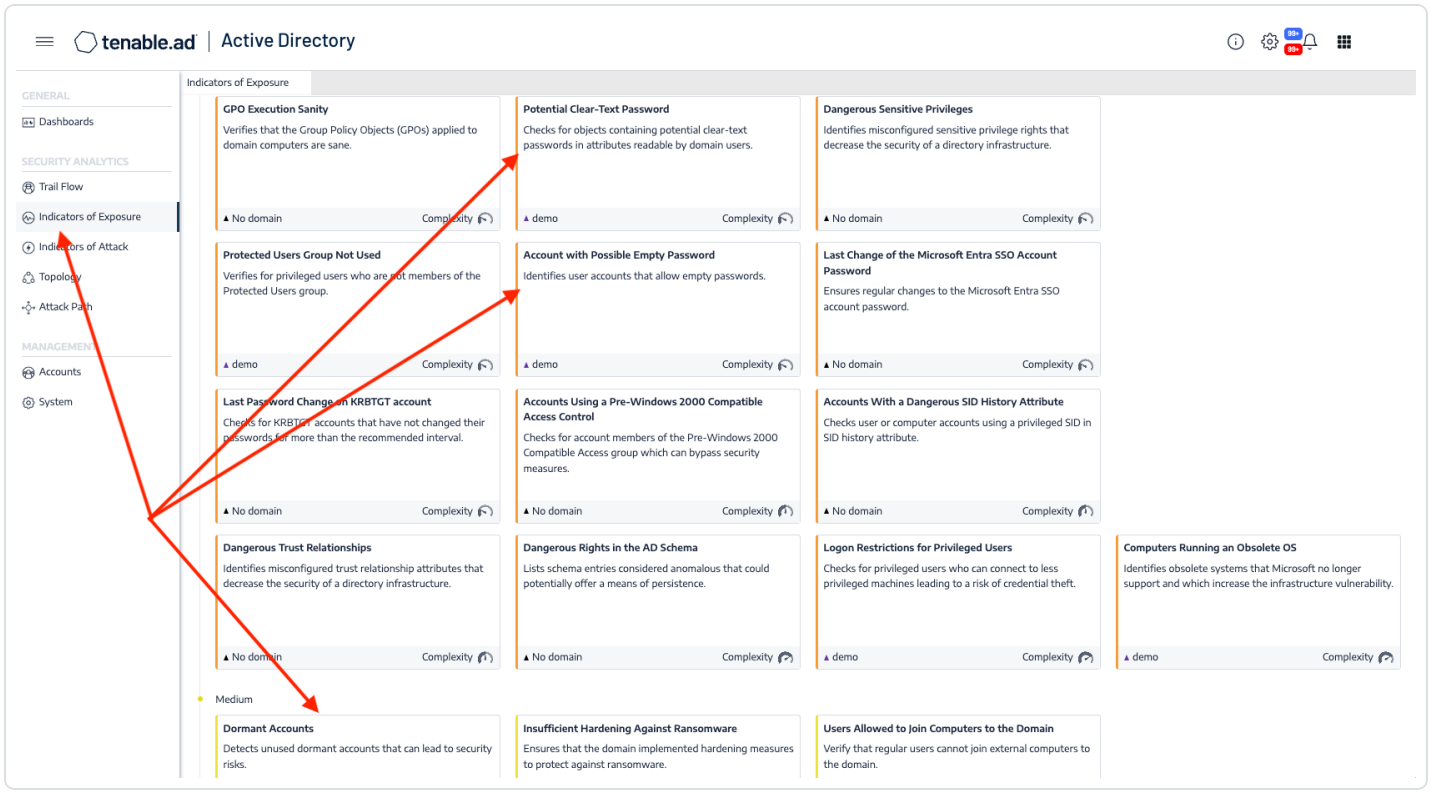
Identity Management

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.



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.

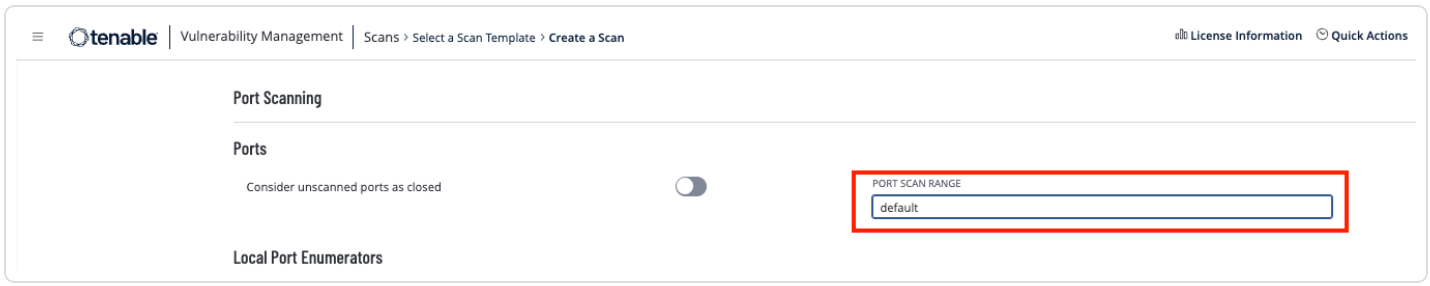
Performing regular software inventory checks also identifies unnecessary software running in the environment, which increases the attack surface without providing a business advantage. In addition, running unnecessary software creates overhead and an inefficient runtime environment. Finally, a software 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.



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.

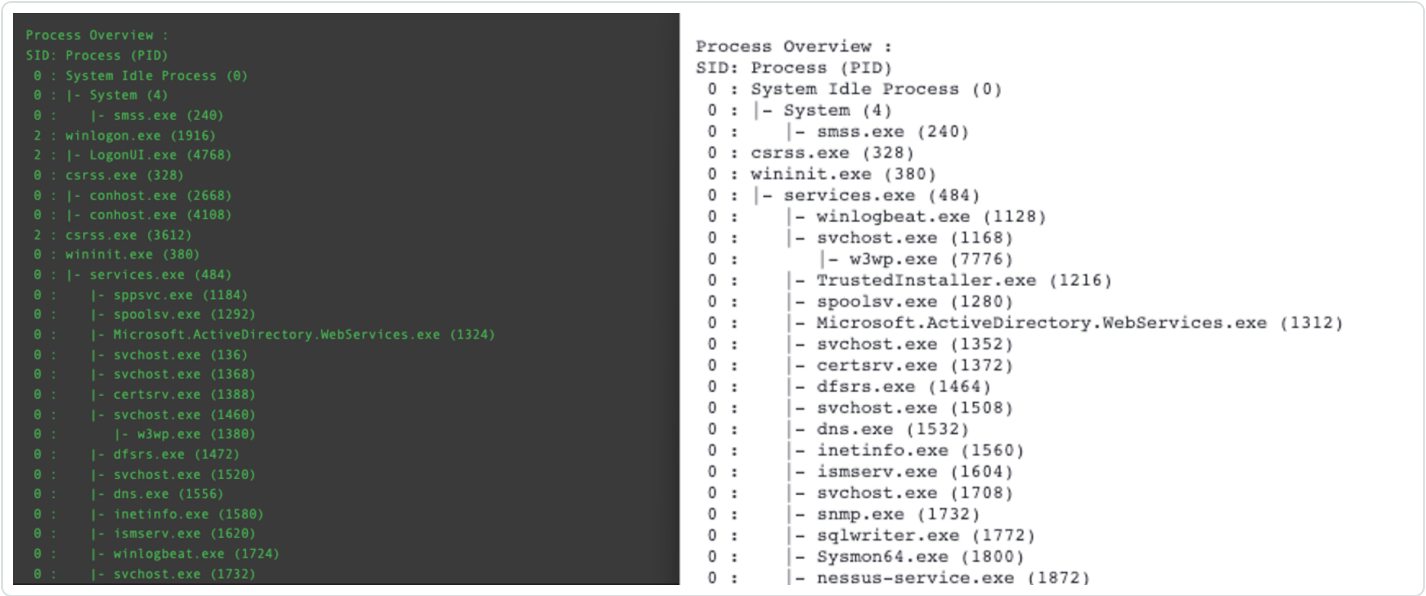
Detecting Services

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.

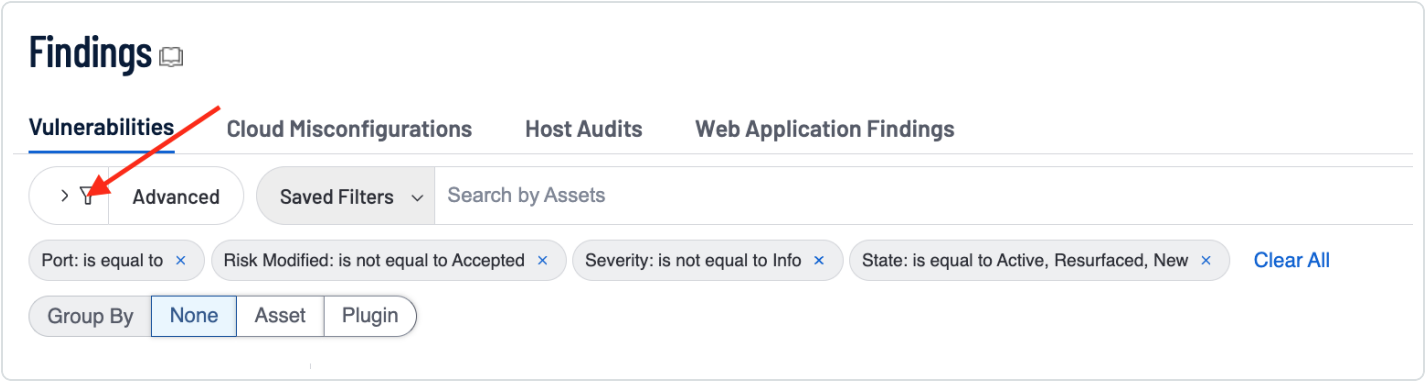


```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- smss.exe (240)
 2 : winlogon.exe (1916)
 2 : |- LogonUI.exe (4768)
 0 : csrss.exe (328)
 0 : |- conhost.exe (2668)
 0 : |- conhost.exe (4108)
 2 : csrss.exe (3612)
 0 : wininit.exe (380)
 0 : |- services.exe (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)
```

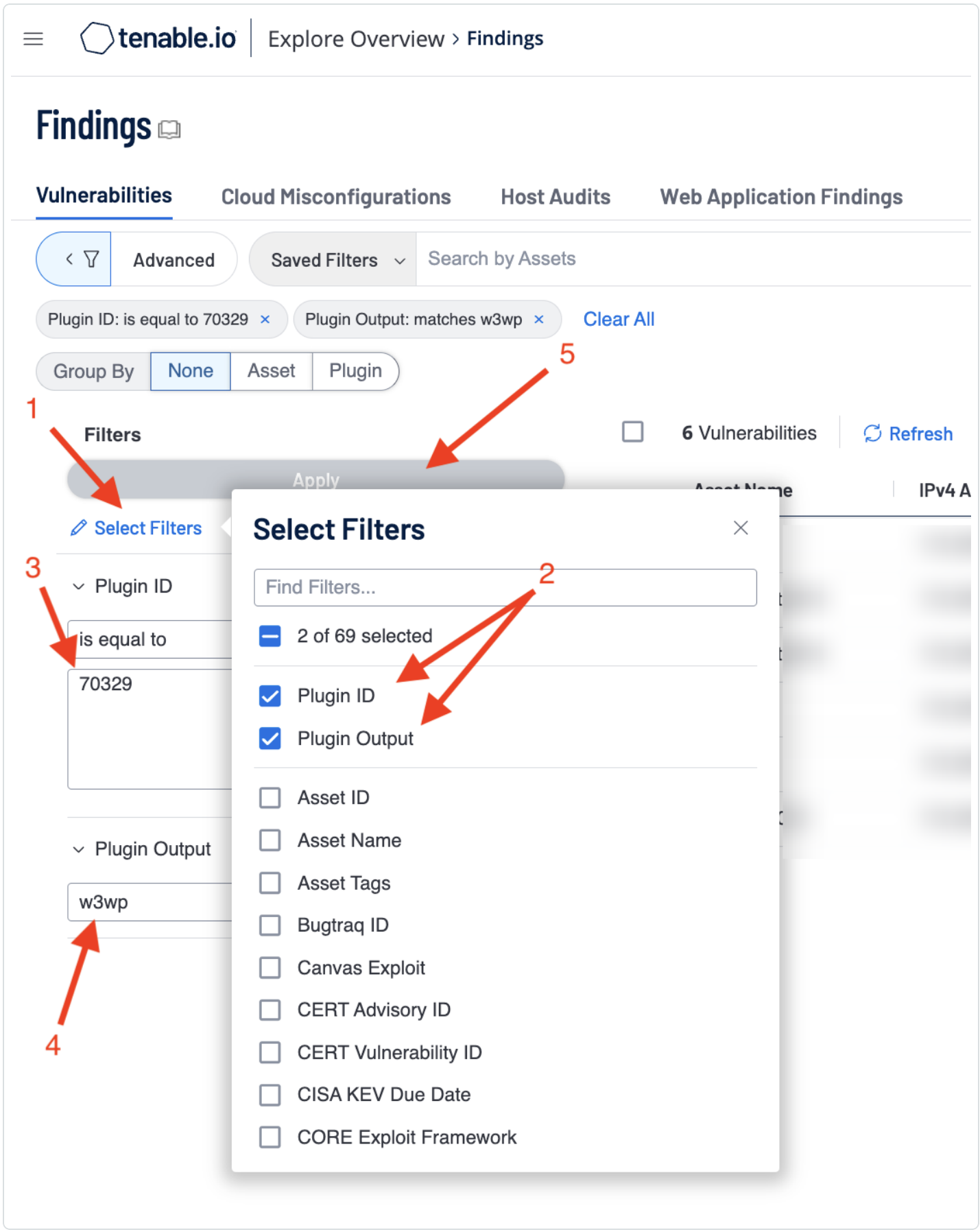
```
Process Overview :
SID: Process (PID)
 0 : System Idle Process (0)
 0 : |- System (4)
 0 :    |- smss.exe (240)
 0 : csrss.exe (328)
 0 : wininit.exe (380)
 0 : |- services.exe (484)
 0 :    |- winlogbeat.exe (1128)
 0 :    |- svchost.exe (1168)
 0 :       |- w3wp.exe (7776)
 0 :    |- TrustedInstaller.exe (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

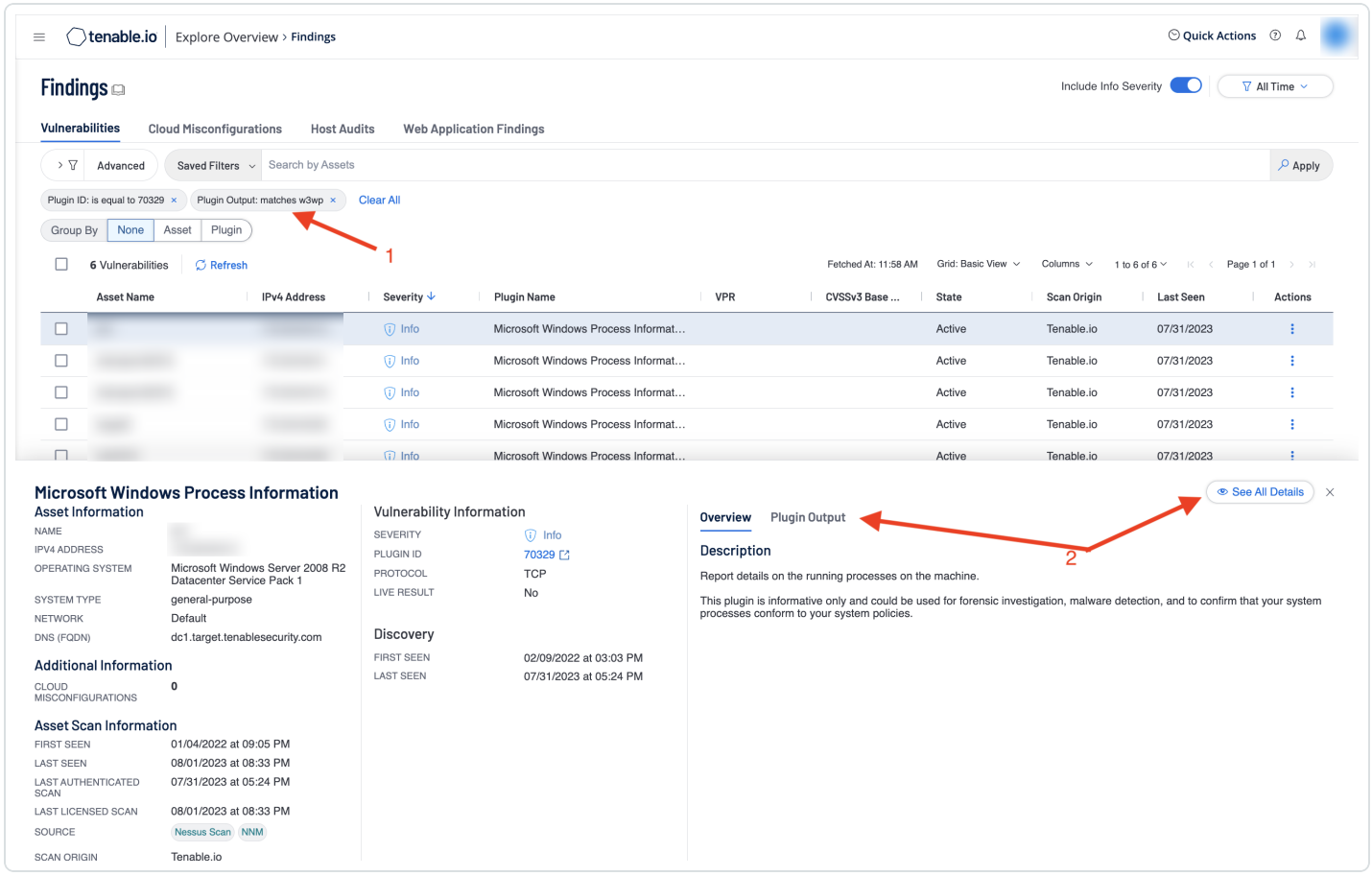
To perform this search in Tenable Vulnerability Management, from the **Findings** page, click on the **Advanced** button and then the filter tab, as shown in the following image:



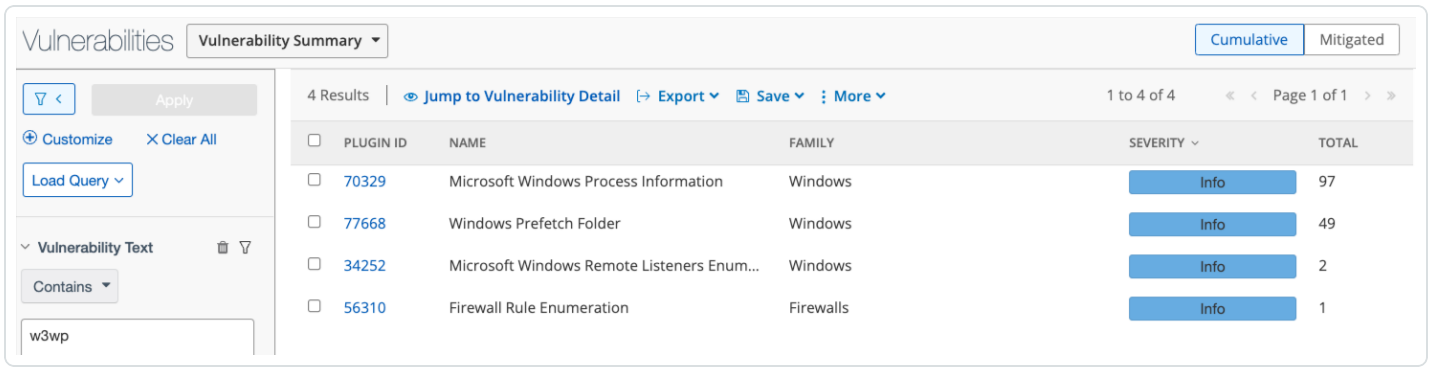
An interface to search based on selected criteria is displayed, as shown in the following image. Click on **Select Filters** (**1**) and select the desired filters for the query. In this example, **Plugin ID** and **Plugin Output** (**2**). Deselect any filters, which are not required for the search, 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.


tenable.io
Explore Overview > Findings
Findings
Vulnerabilities
Cloud Misconfigurations
Host Audits
Web Application Findings
Advanced
Saved Filters
Search by Assets
Plugin ID: is equal to 70329
Plugin Output: matches w3wp
Clear All
Group By
None
Asset
Plugin
1
Filters
6 Vulnerabilities
Refresh
Apply
5
Select Filters
Select Filters
3
Plugin ID
is equal to
70329
Find Filters...
2
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 Output
w3wp
4
IPv4 A

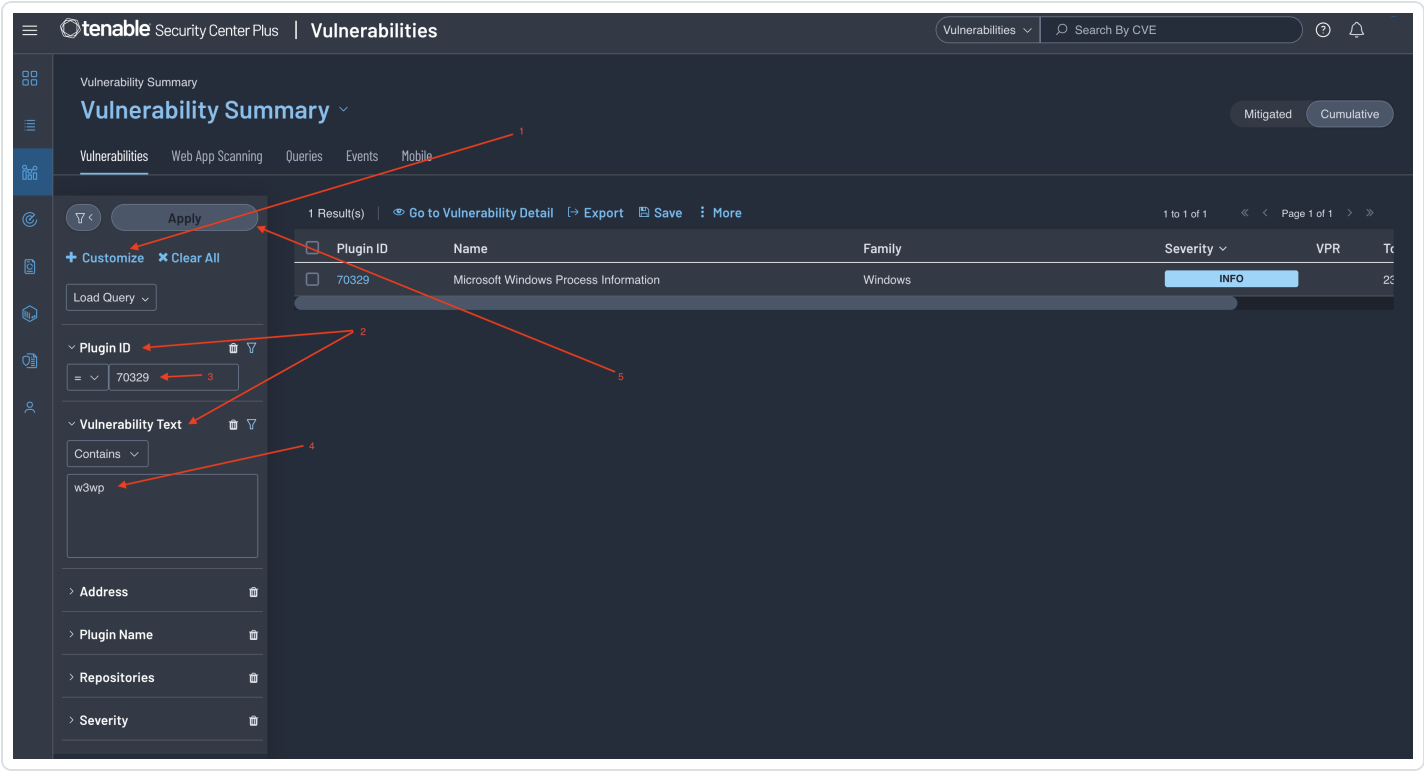
The search results page is displayed showing all assets containing the search query filter. For this example, the **Plugin ID** and **Plugin Output** (**1**) are shown. Clicking on a result displays summary information of the results. More details, including the Plugin Output can be found by clicking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



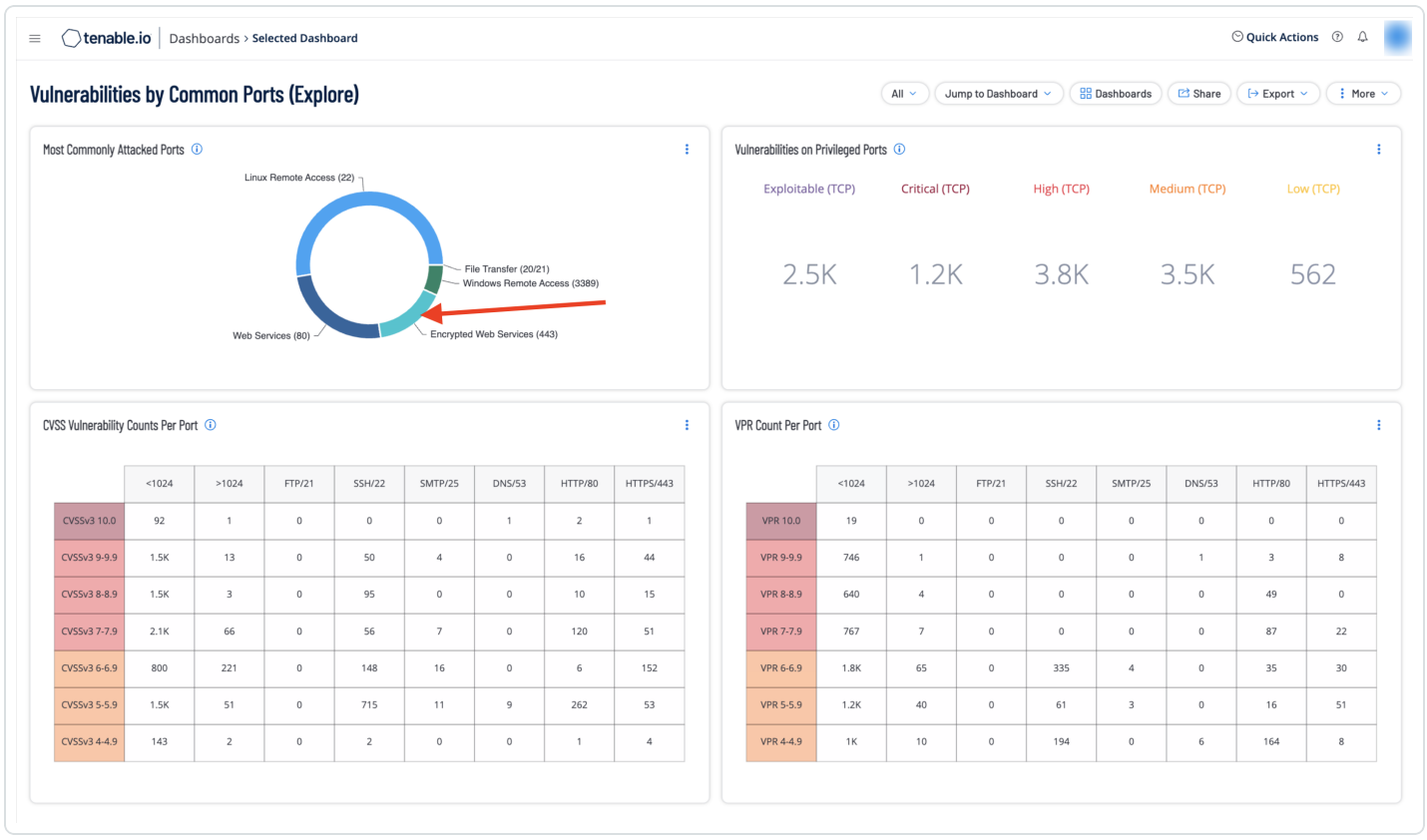
The search can be pivoted from Plugin ID to Vulnerability Text. The following image displays all other scan results containing “w3wp” in the plugin output (vulnerability text). This information can now be investigated using the **Vulnerability Detail List** tool or the **Vulnerability List** tool in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



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.



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.

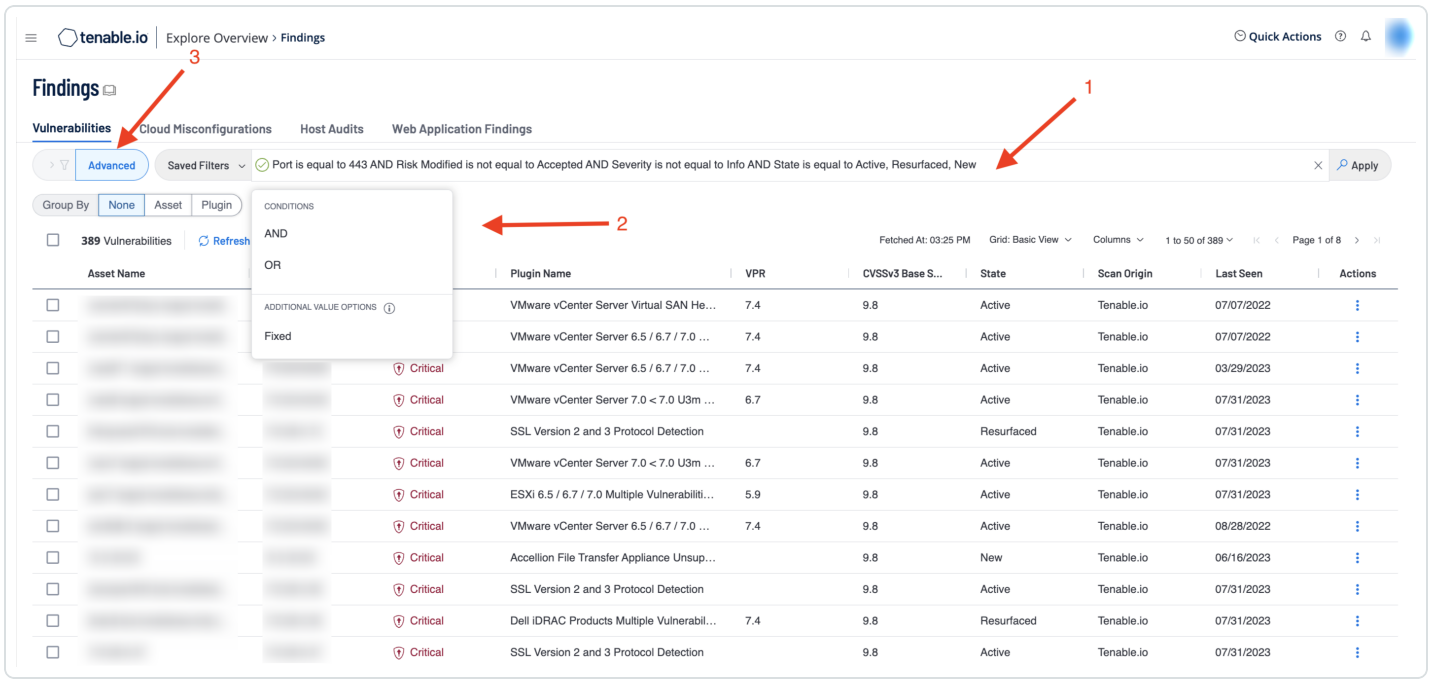


	<1024	>1024	FTP/21	SSH/22	SMTP/25	DNS/53	HTTP/80	HTTPS/443
CVSSv3 10.0	92	1	0	0	0	1	2	1
CVSSv3 9-9.9	1.5K	13	0	50	4	0	16	44
CVSSv3 8-8.9	1.5K	3	0	95	0	0	10	15
CVSSv3 7-7.9	2.1K	66	0	56	7	0	120	51
CVSSv3 6-6.9	800	221	0	148	16	0	6	152
CVSSv3 5-5.9	1.5K	51	0	715	11	9	262	53
CVSSv3 4-4.9	143	2	0	2	0	0	1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

	<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

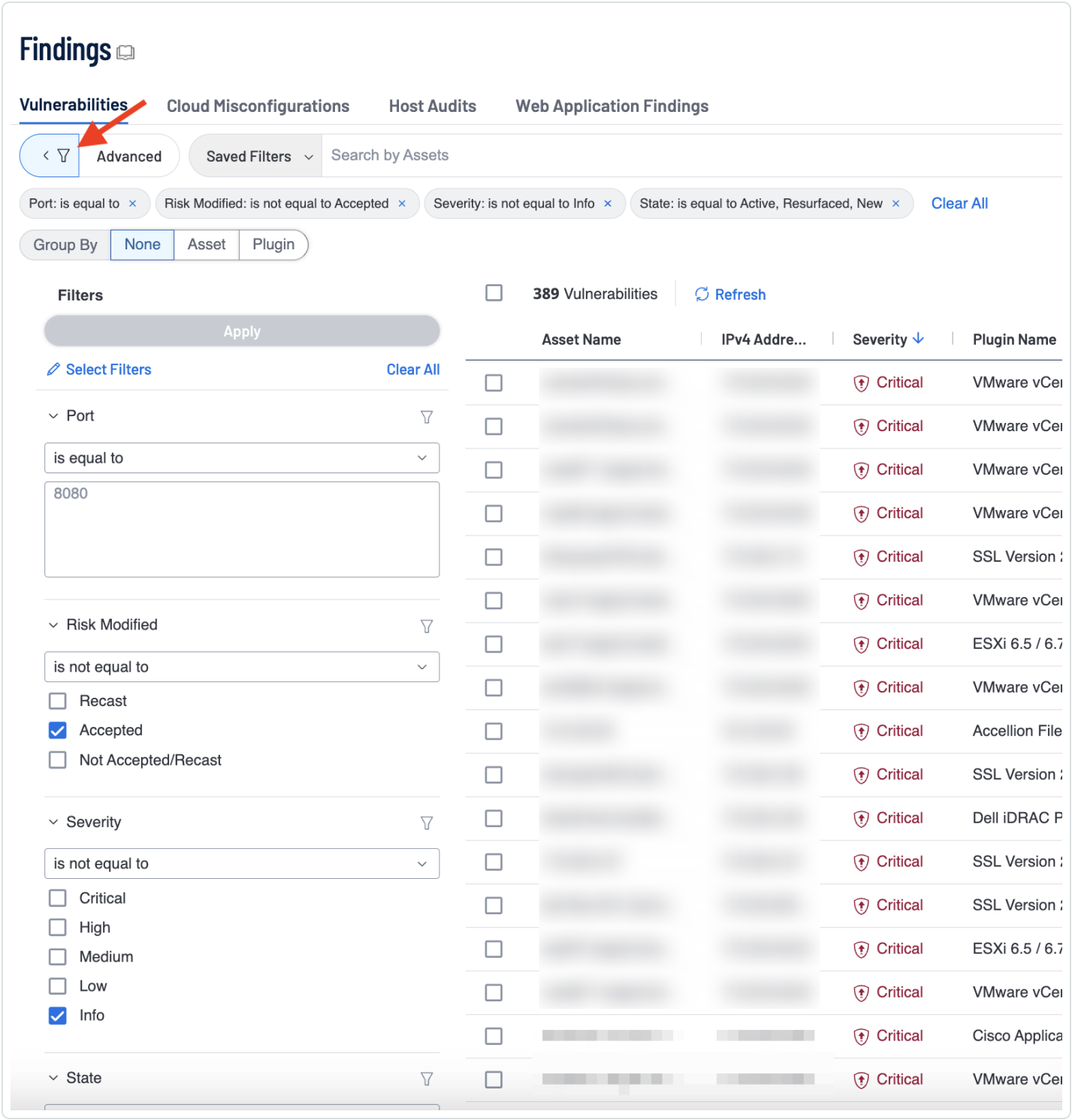
Additional filtering can be performed from either the Conditions field (**1**) or the Advanced (**3**) button. Clicking on the Conditions field opens the Conditions menu (**2**) to refine the filter search.



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**).

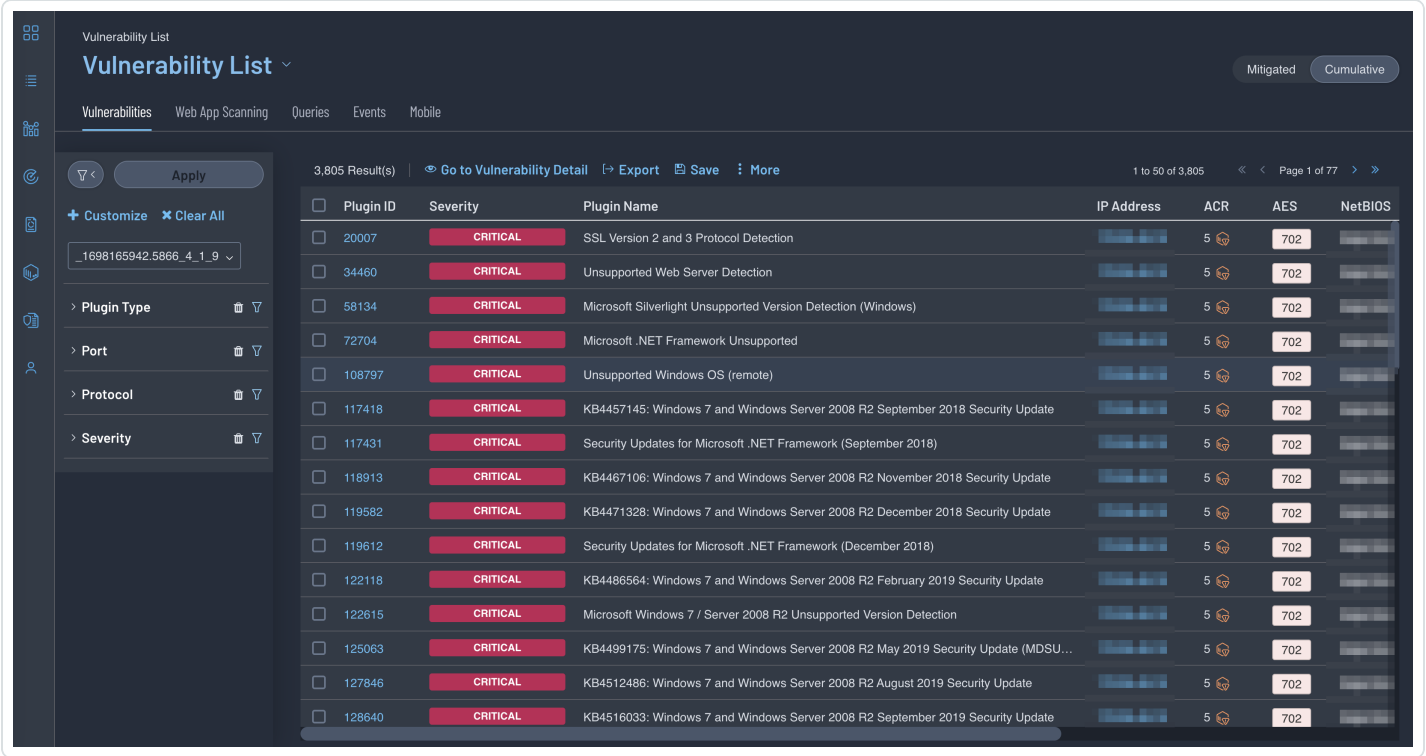
Additional conditions can be added (**1**) or the filter can be applied by clicking on the **Apply** (**2**) button, as shown in the following image:

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:

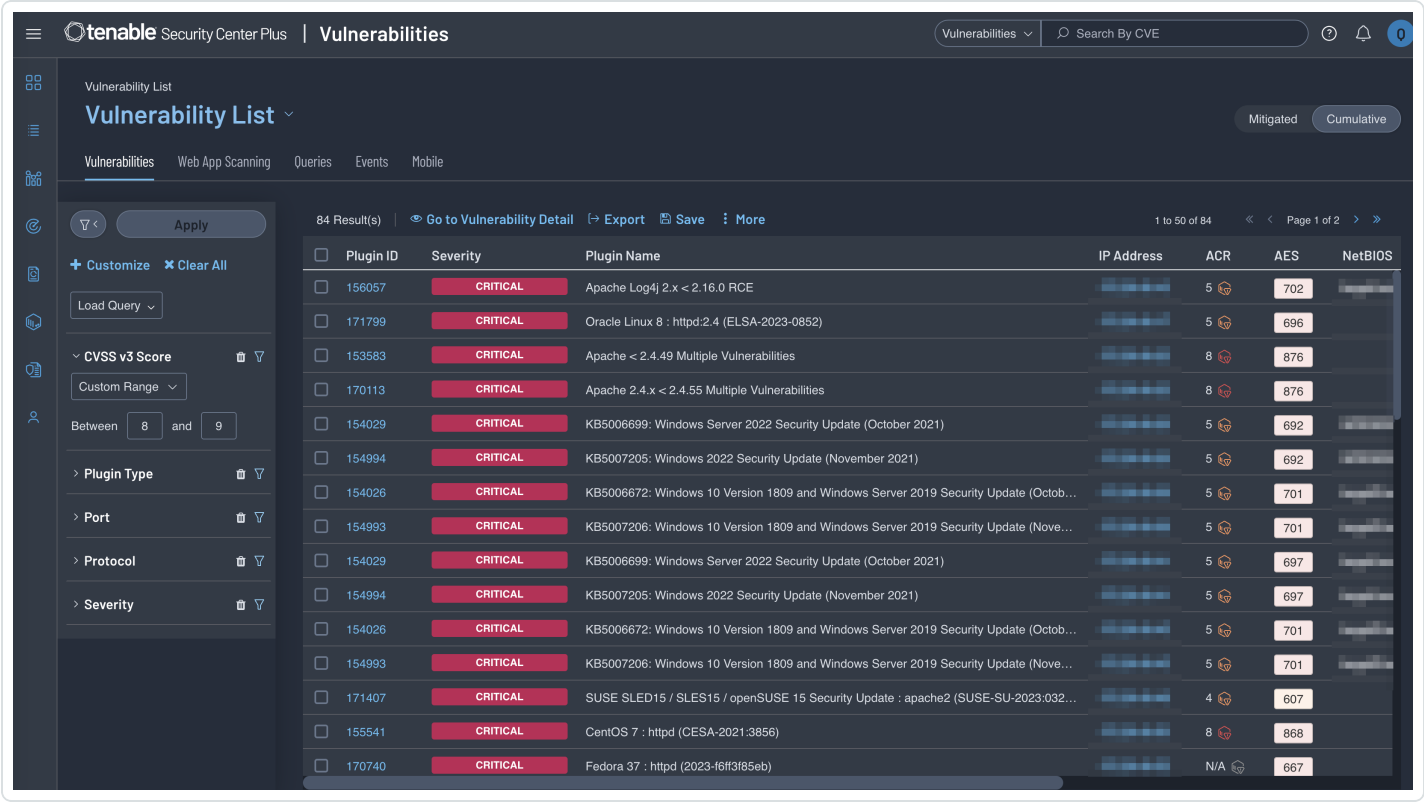


Drilling Down in Tenable Security Center

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.



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

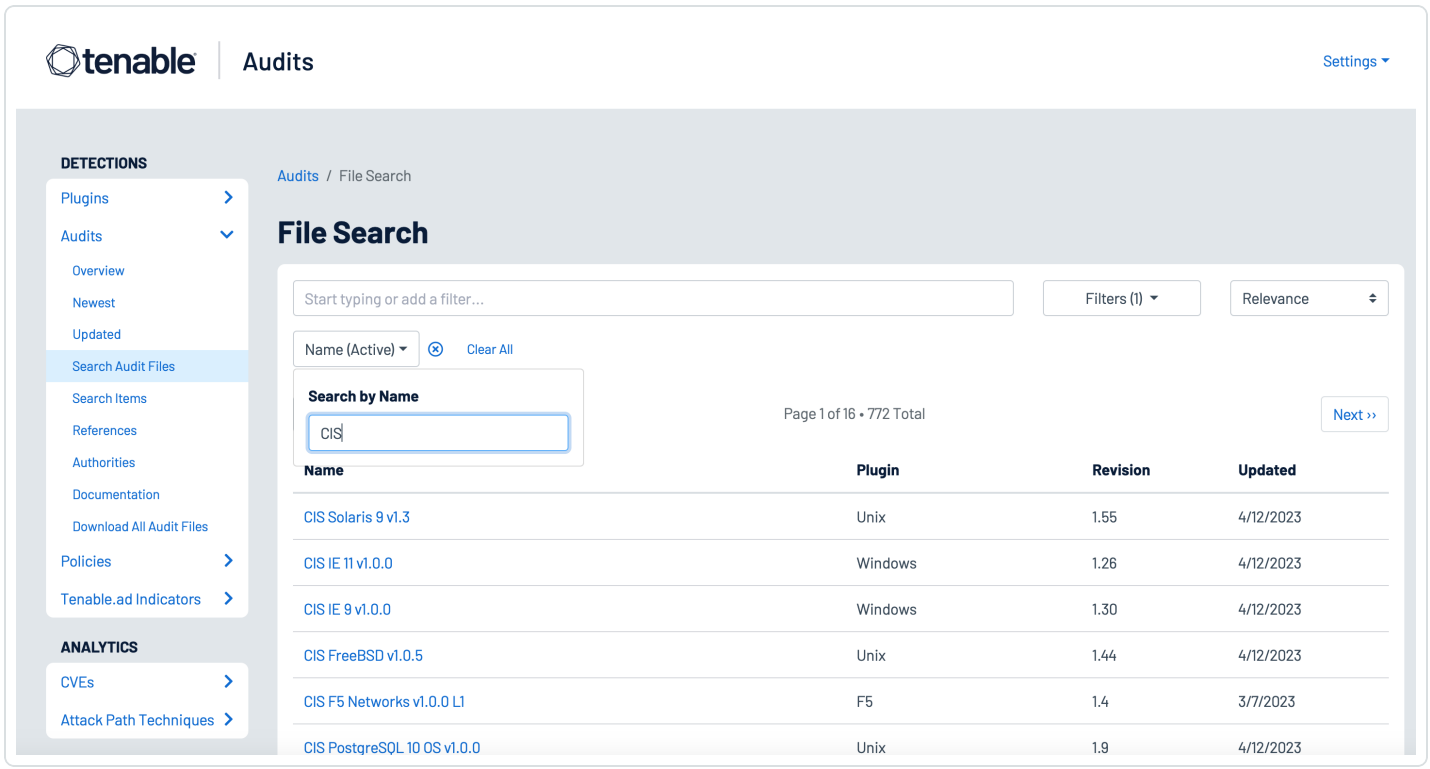


Application Server Hardening

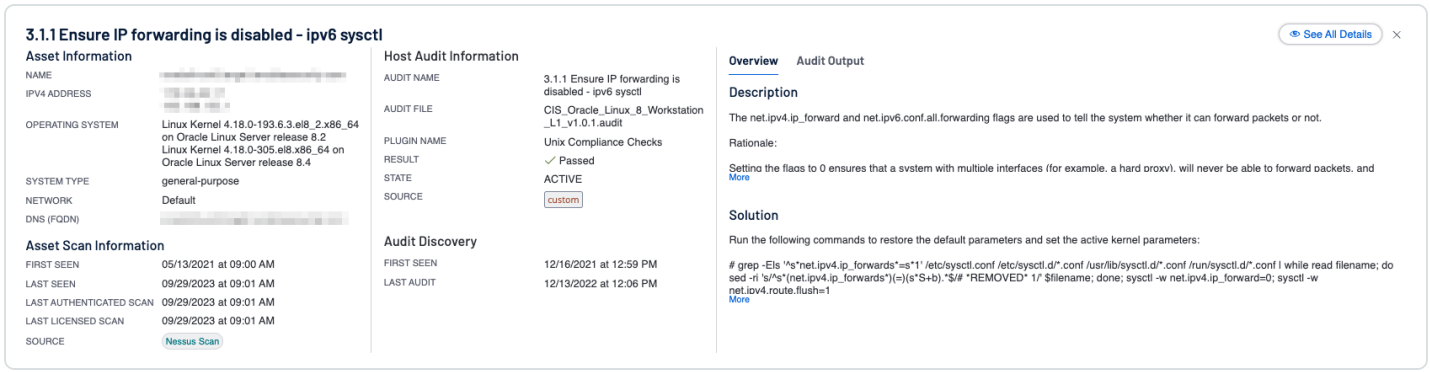
Application server hardening is the process of securing and fortifying an application server to reduce the device's exposure to potential threats and vulnerabilities. Even if an application is written following the best application security practices, the application can still be vulnerable if the server 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.

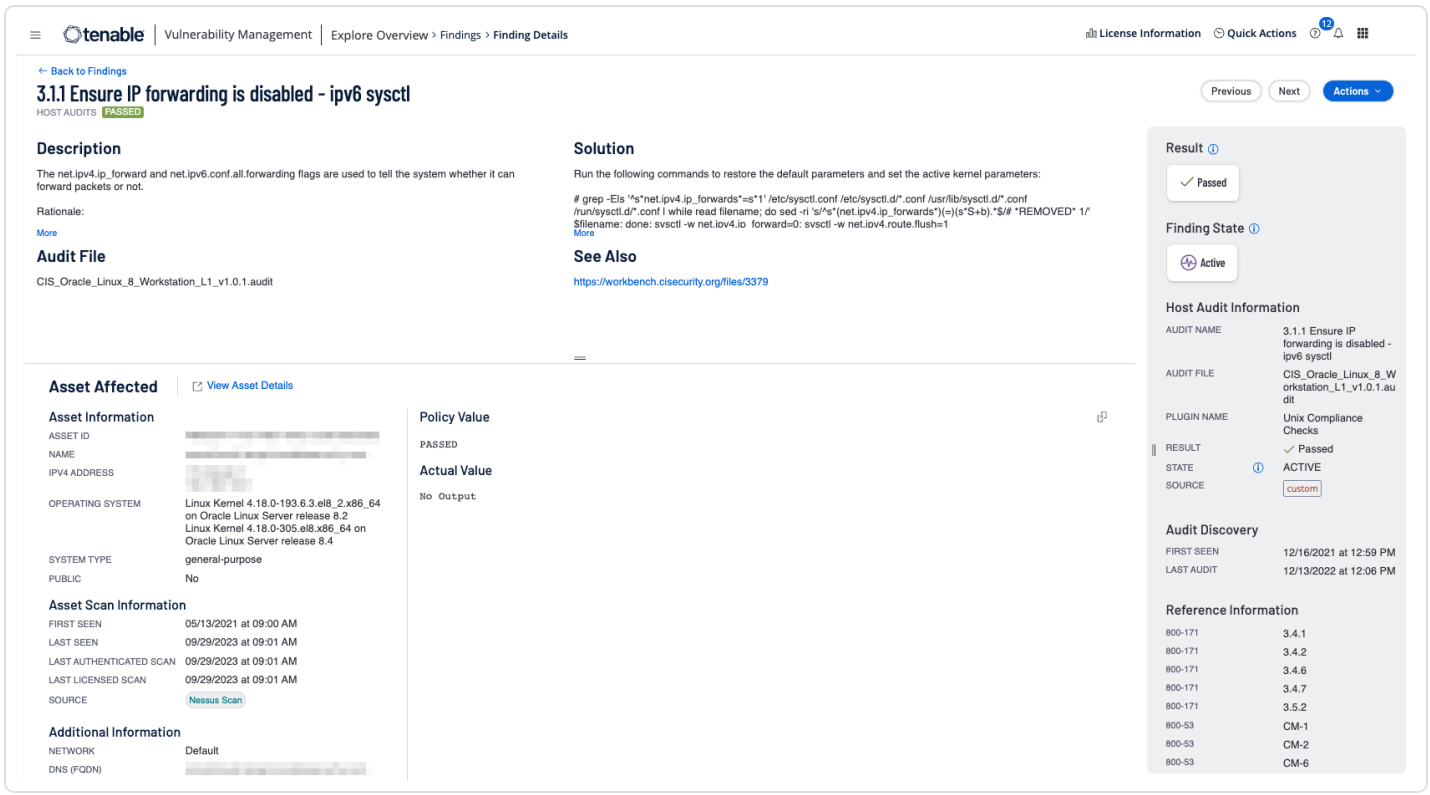
Compliance scanning is accomplished by conducting compliance checks using specific audit files and privileged credentials added to the scan policy. Use the Tenable Audit Search page with the Name filter to search for system hardening audits, such as the CIS Benchmarks, as shown in the following image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



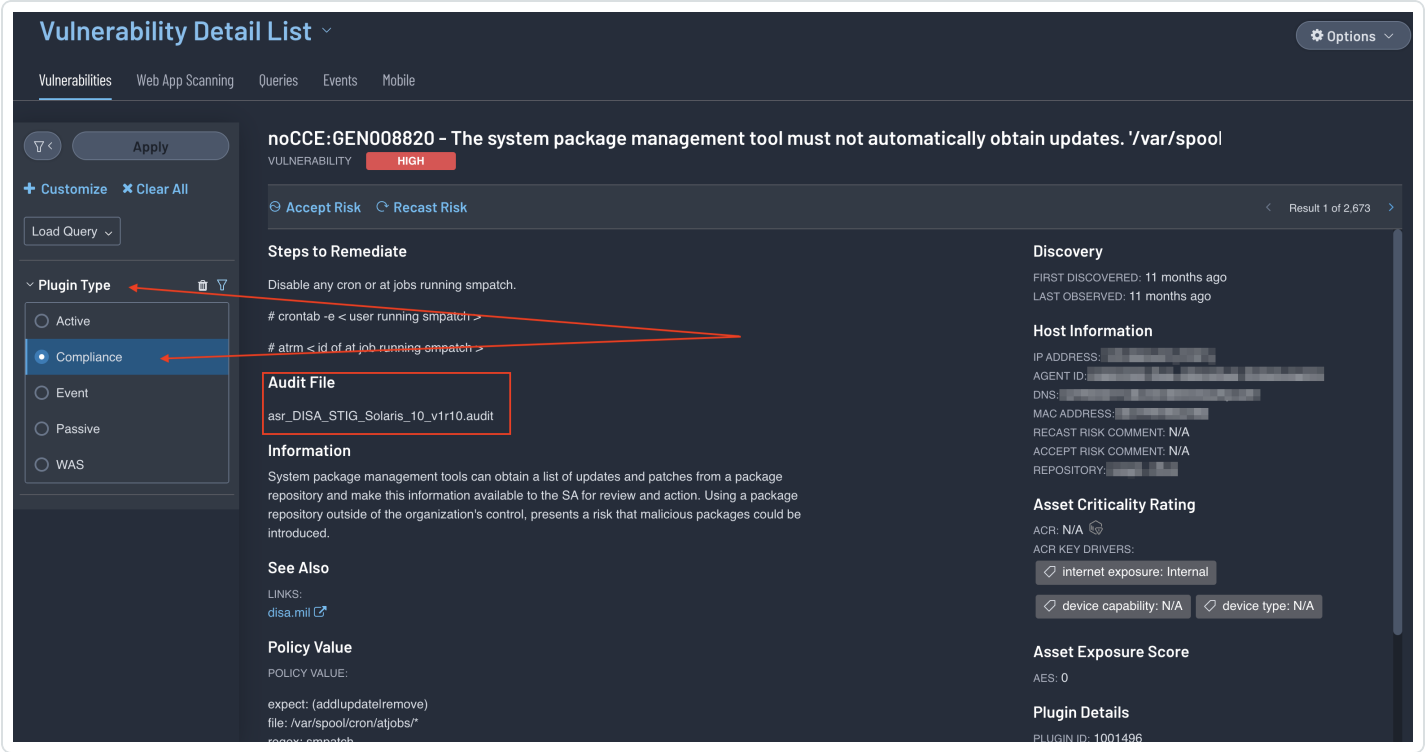
Host audit findings details can be found on the **Findings** page within Tenable Vulnerability Management. Click on a host audit finding to preview the details in the panel.



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



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:

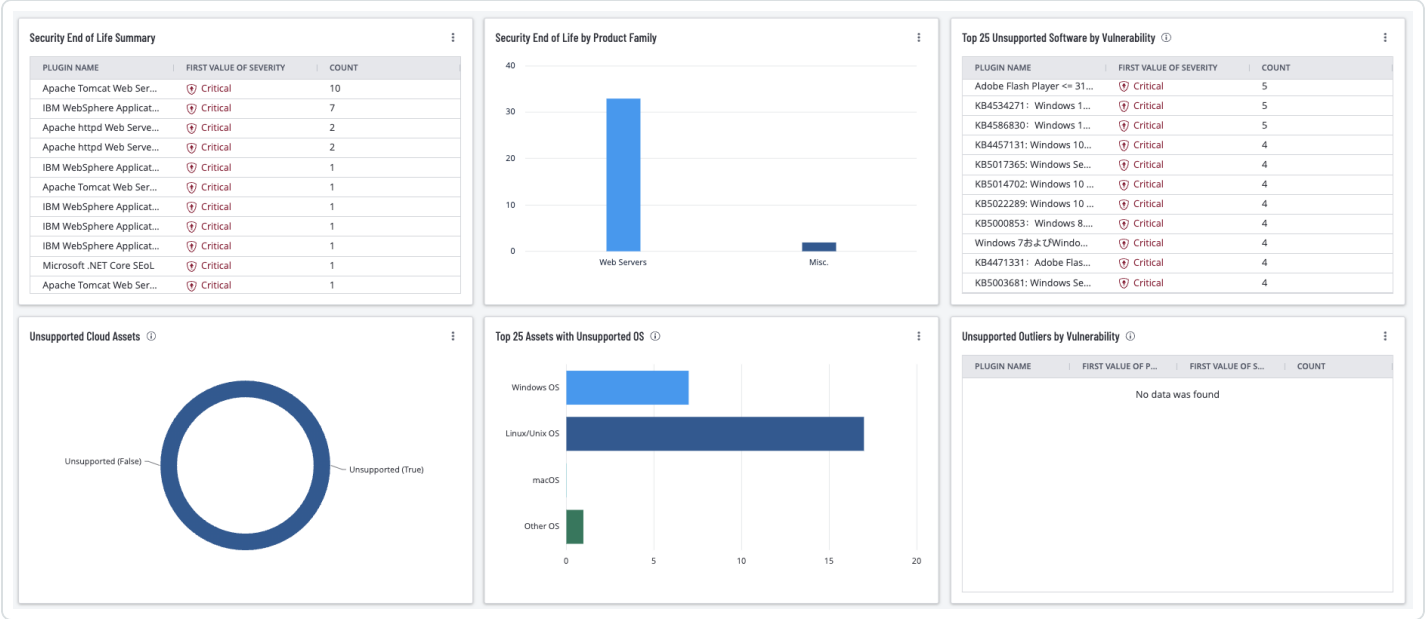


Unsupported Software

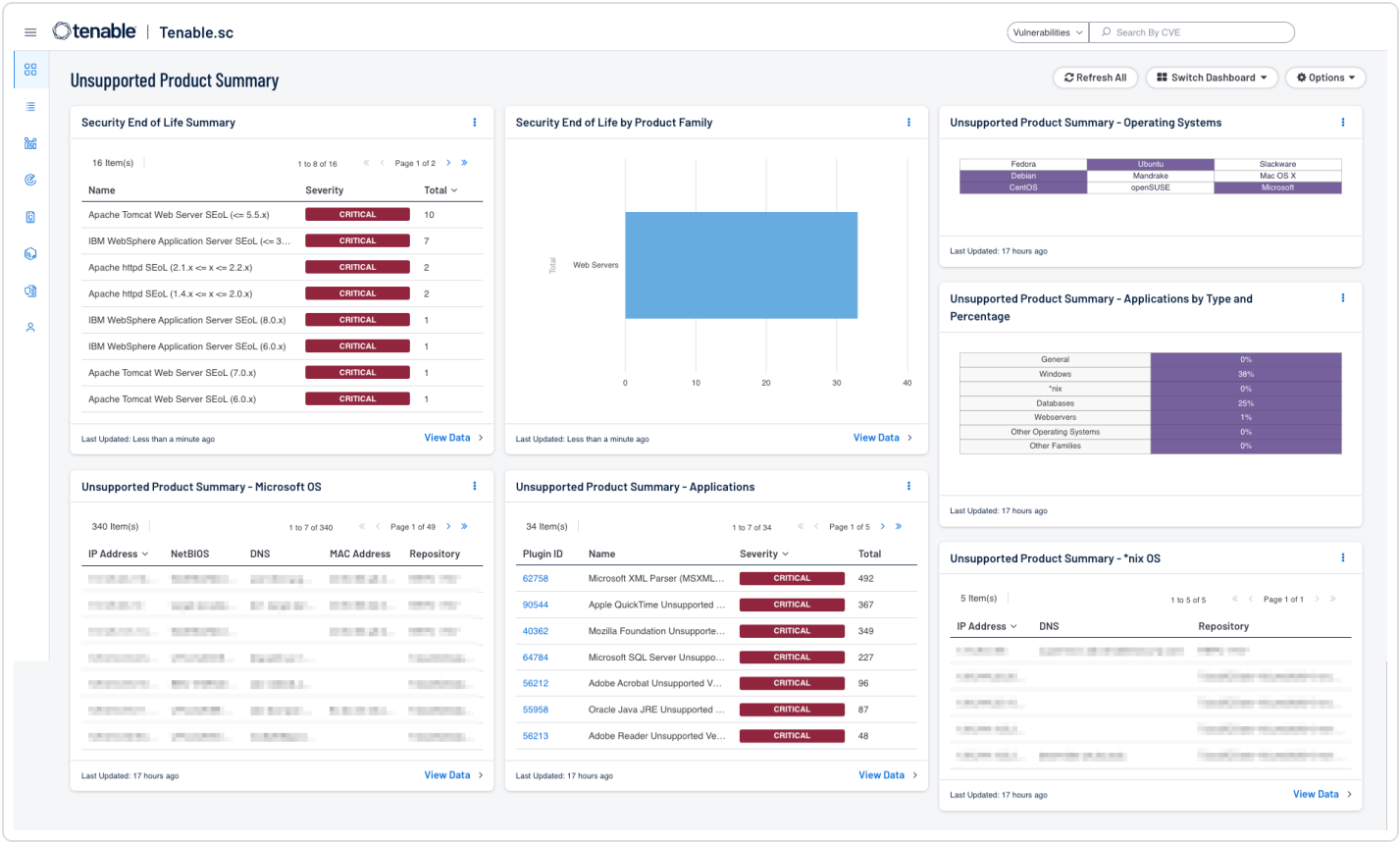
Identifying assets running End of Life (EOL) applications is an important part of assessing and minimizing organizational risk since patches, updates, and security fixes are no longer available. Many standards state organizations must ensure that only software applications or operating systems that are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



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

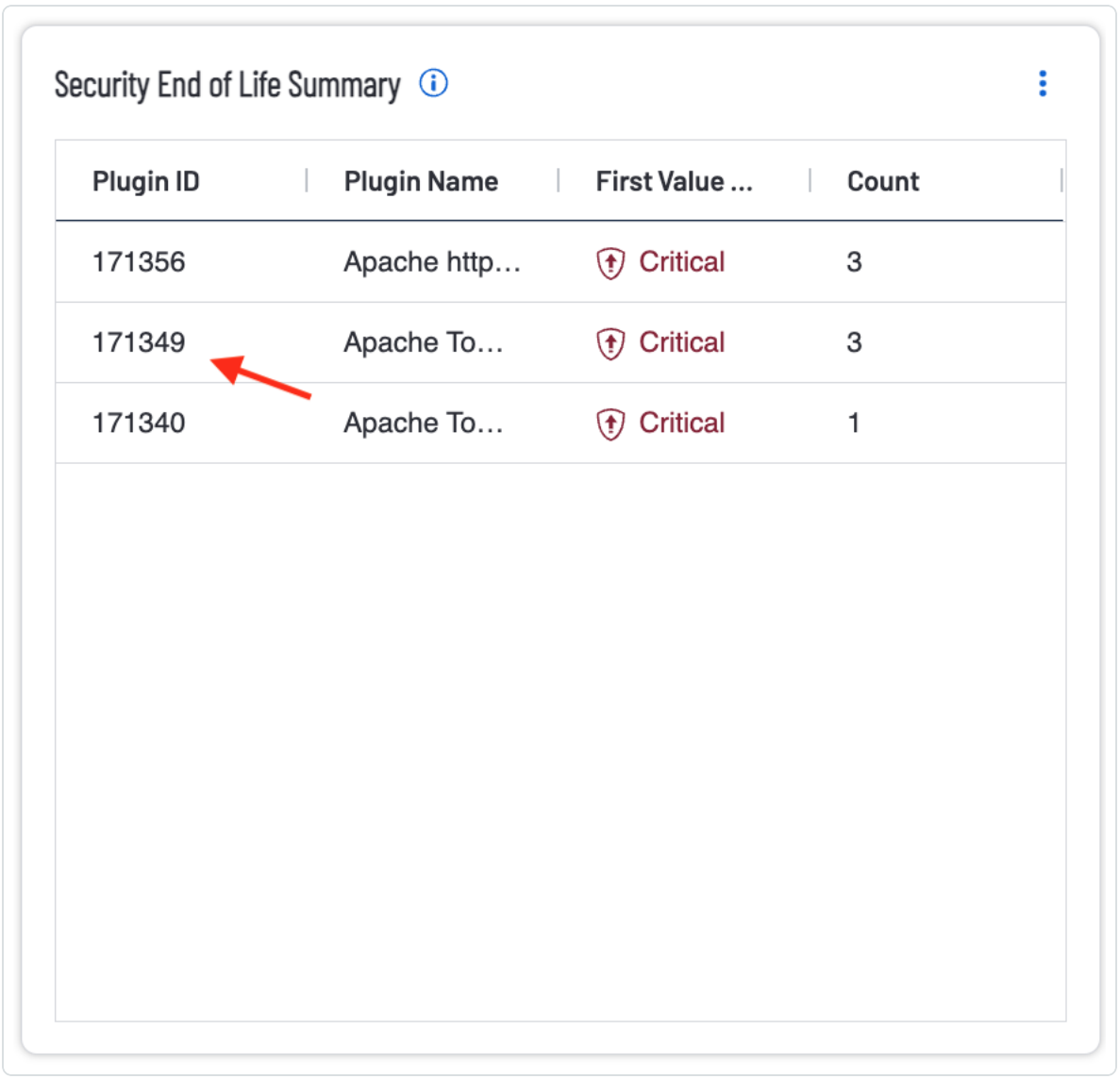


Security End of Life

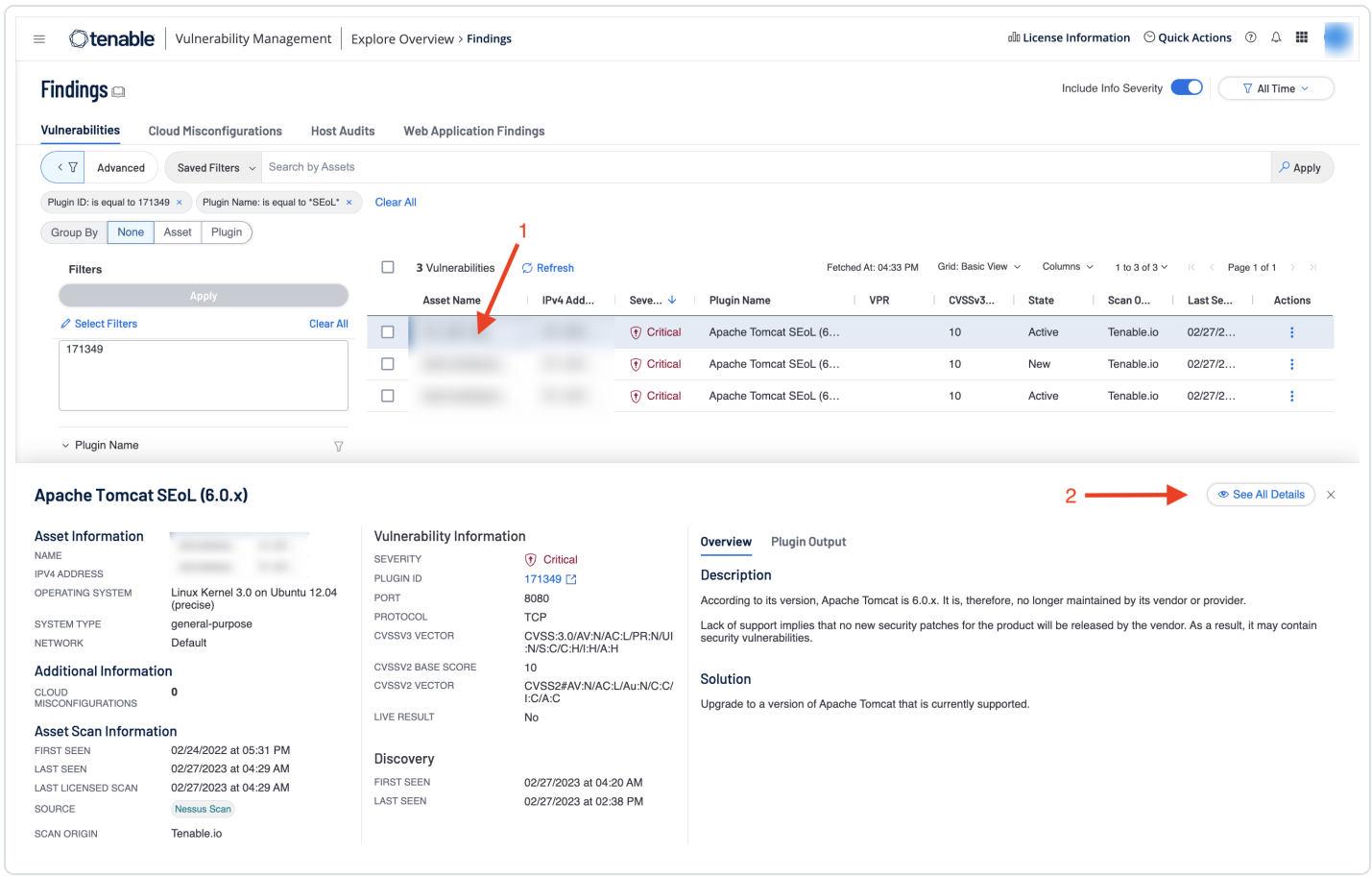
The **Security End of Life** widget (Tenable Vulnerability Management) and the **Security End of Life Summary** component (Tenable Security Center) displays information about products that have entered the Security End of Life state of the Security Maintenance Lifecycle. This component utilizes a filter 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

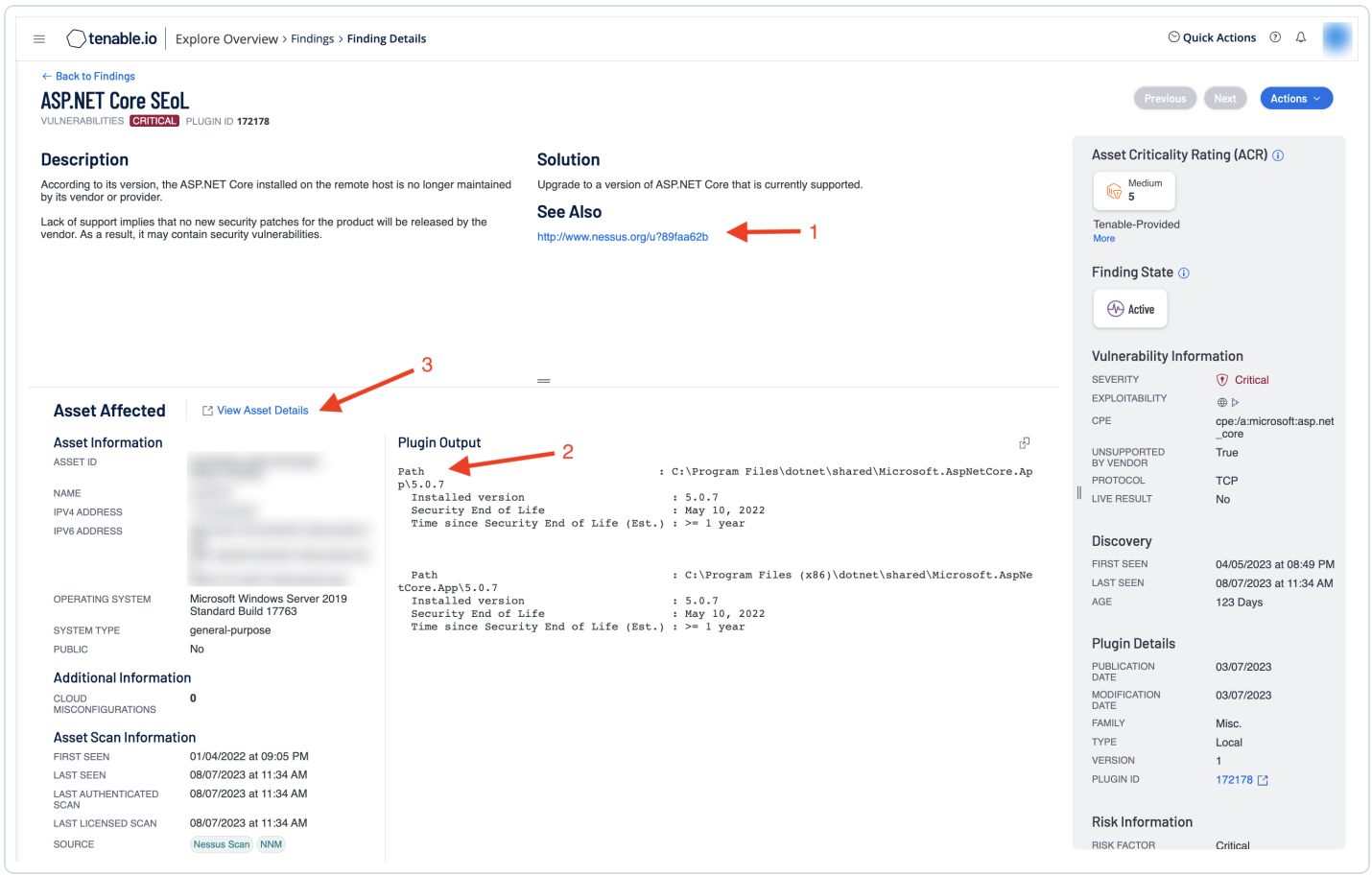
Drilling down into the data presents a vulnerability summary where additional details on each identified SEoL finding can be viewed. Click on a cell to drill into the Findings page for more details and to perform refined searches.



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



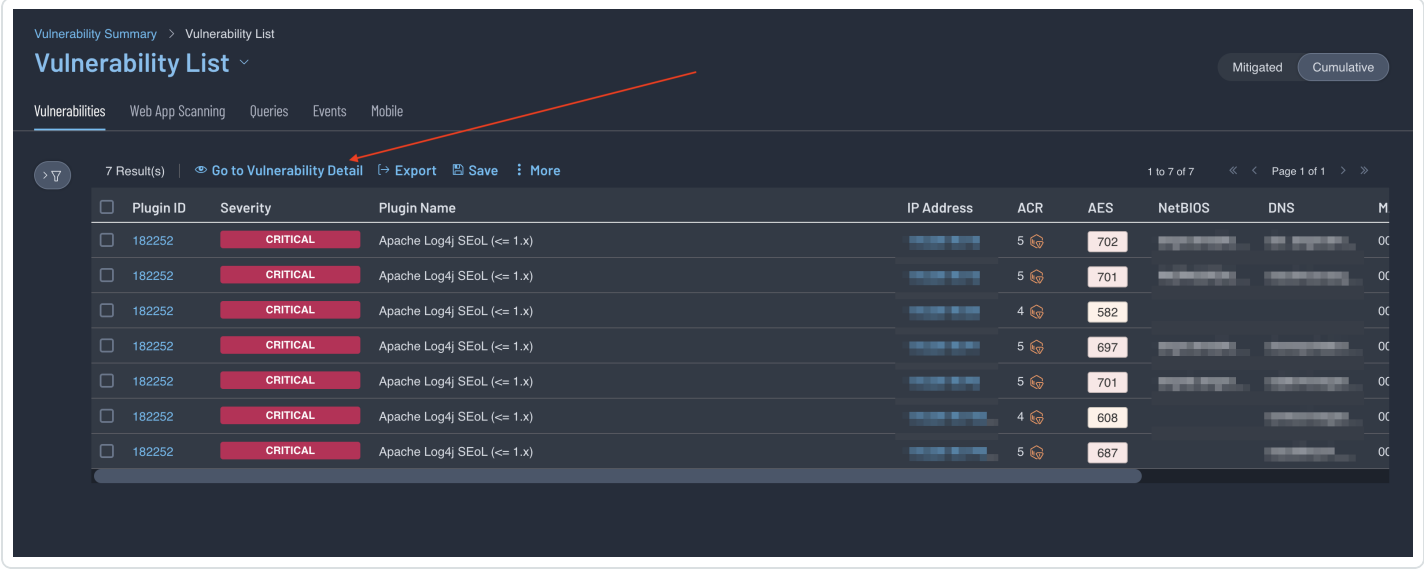
This page contains a lot of useful information, such as a link to additional resources (**1**), the path to the out-of-date application (**2**), and details about the affected asset (**3**).



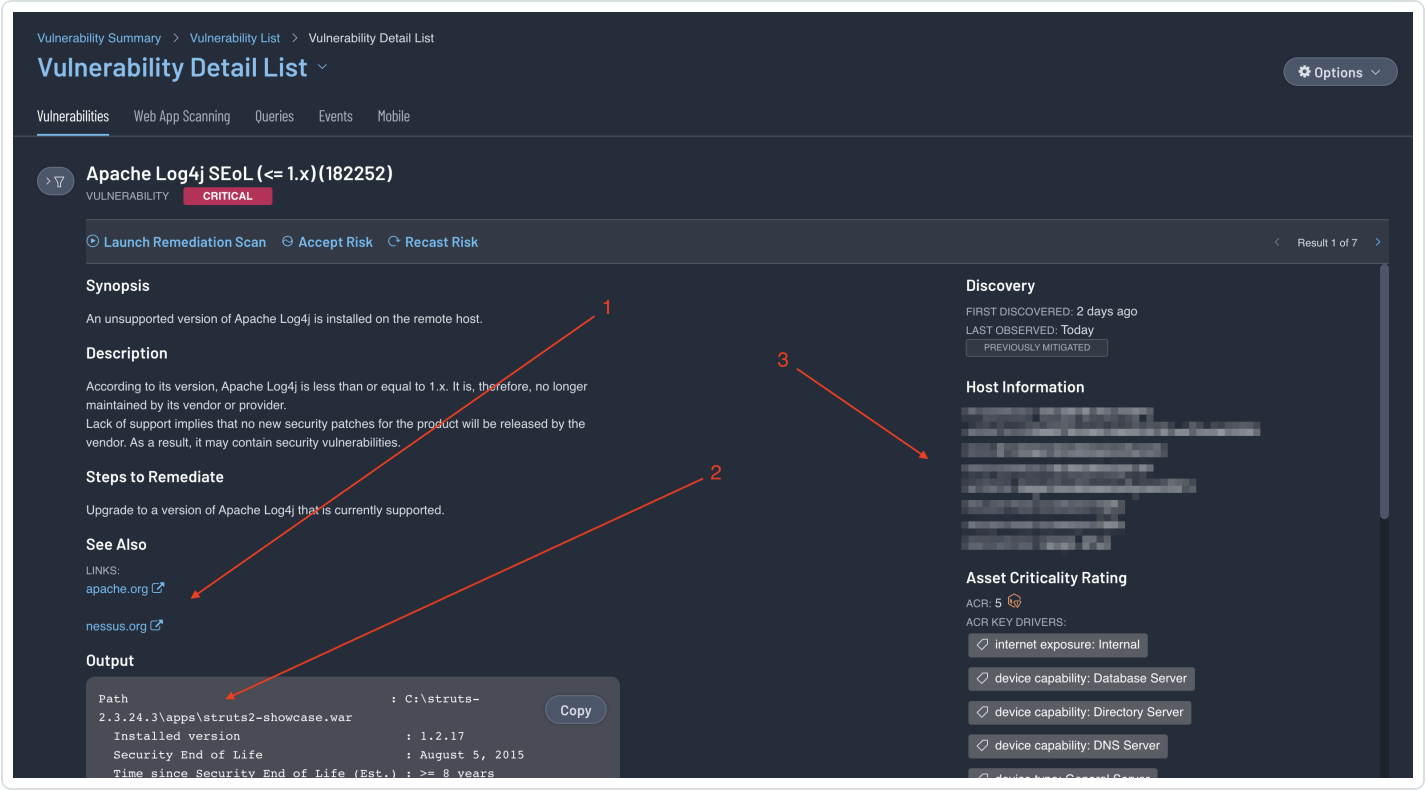
Drill Down for Tenable Security Center

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.

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

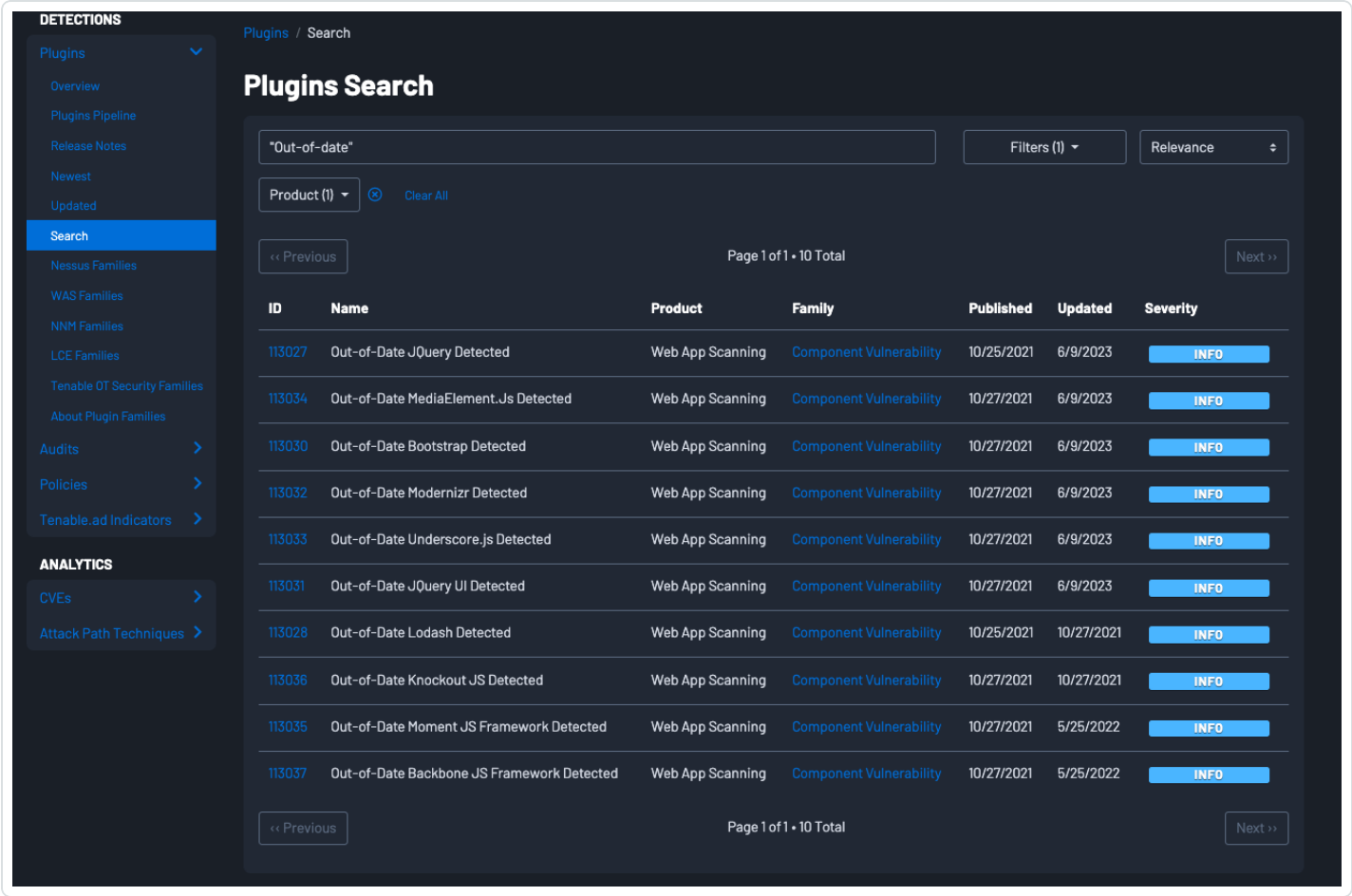


This page contains a lot of useful information, such as a link to additional resources (**1**), the path to the out-of-date application (**2**), and details about the affected asset (**3**).



Out-of-Date Libraries

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



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.

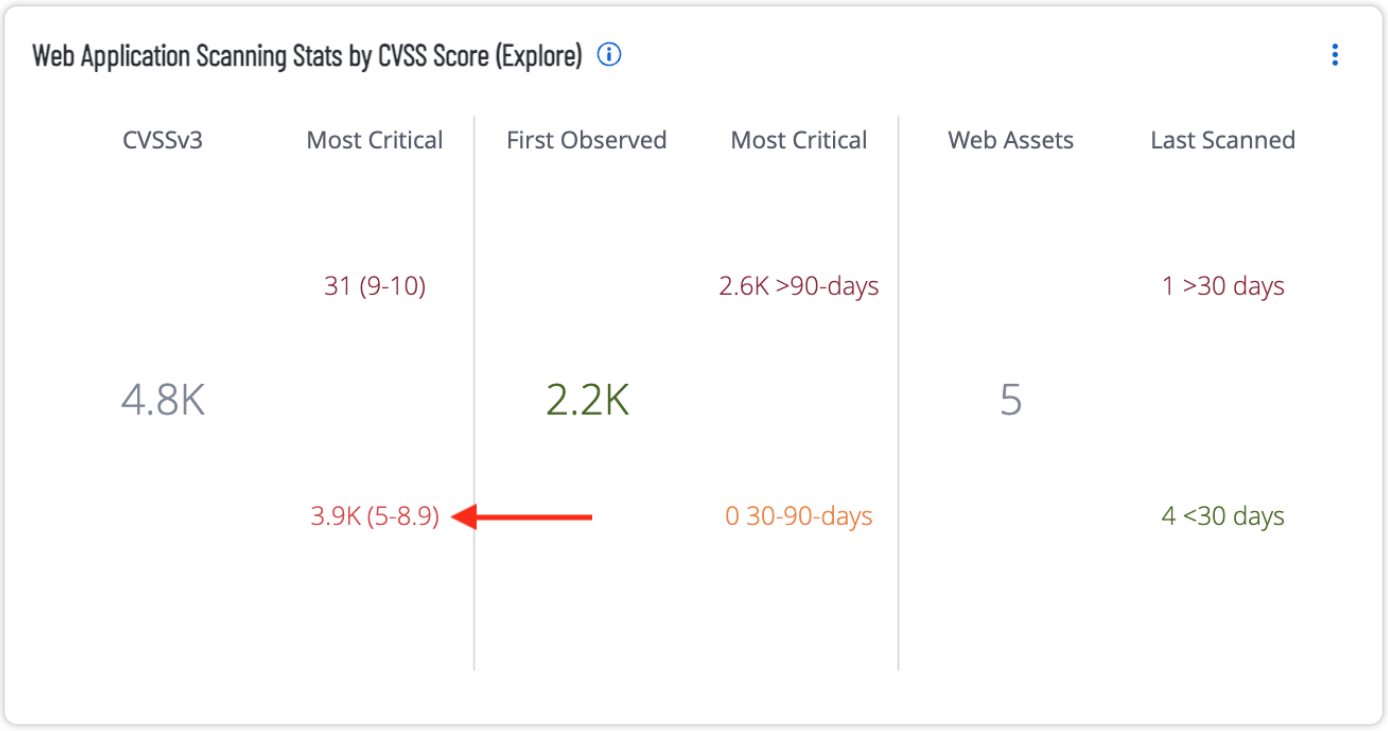
Vulnerabilities by Severity

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.

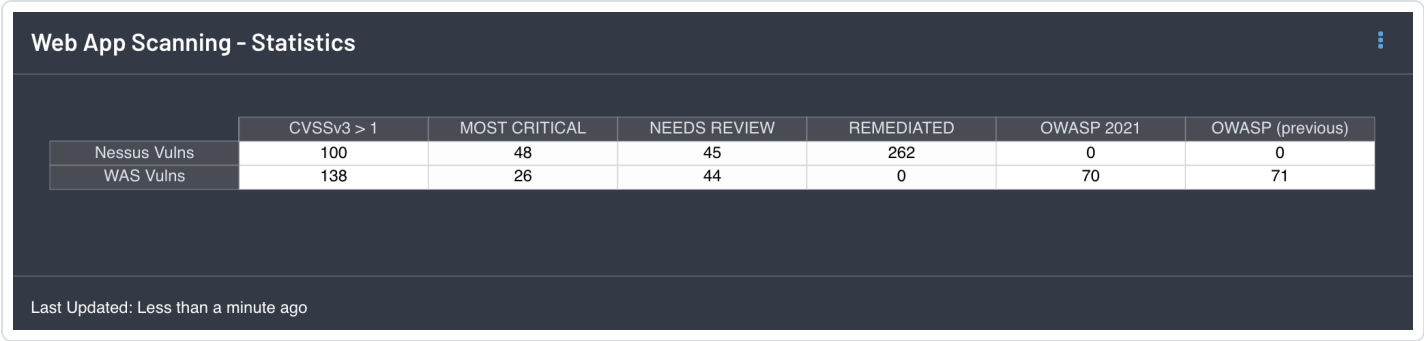
Severity	CVSSv2 Range	CVSSv3 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.	The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.	The plugin's highest vulnerability CVSSv3 score is 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.



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.



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

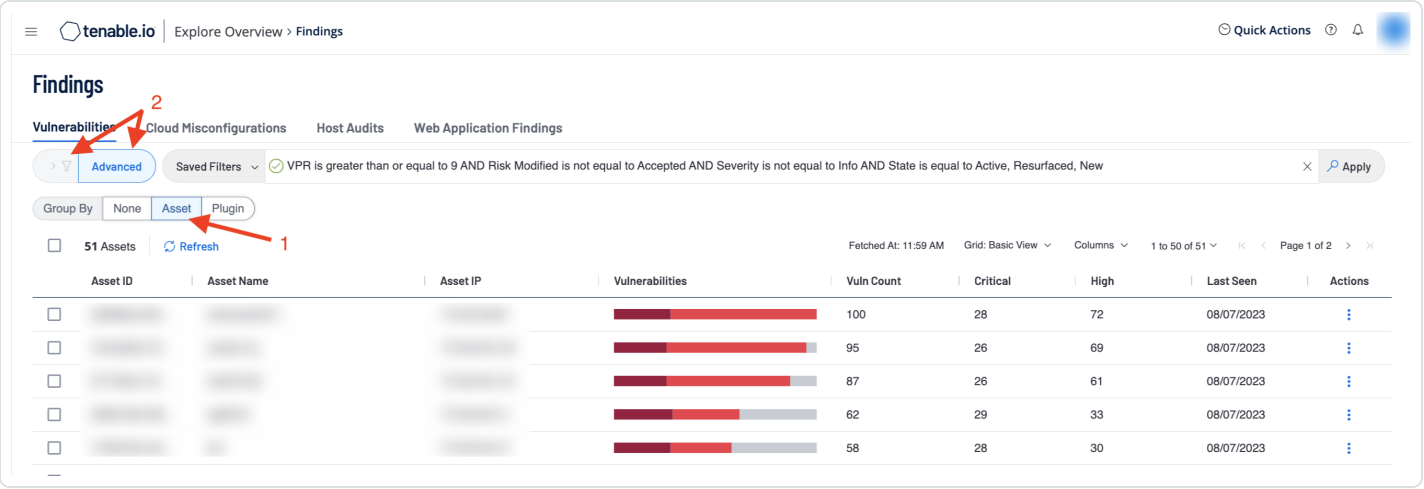
external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (High, Functional, PoC, or Unproven) parallel the CVSS Exploit Code Maturity categories.

- **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.

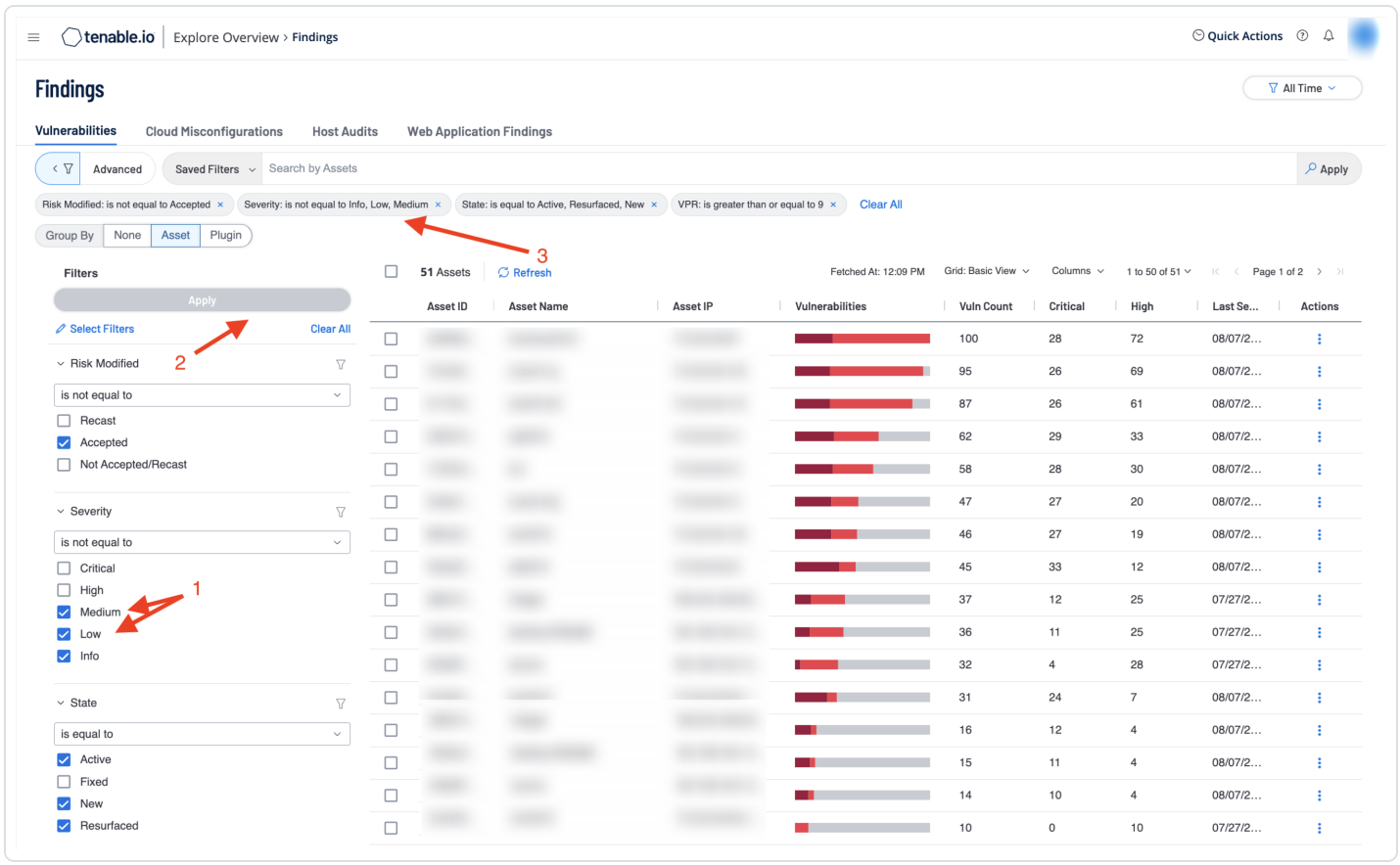
The **Vulnerability Priority Rating Using VPR** widget for Tenable Vulnerability Management displays the vulnerability count, organized by Vulnerability Priority Rating (VPR) category from the traditional vulnerability scans collected using Nessus scanners. VPR is a dynamic metric representing the likelihood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

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**).



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**).



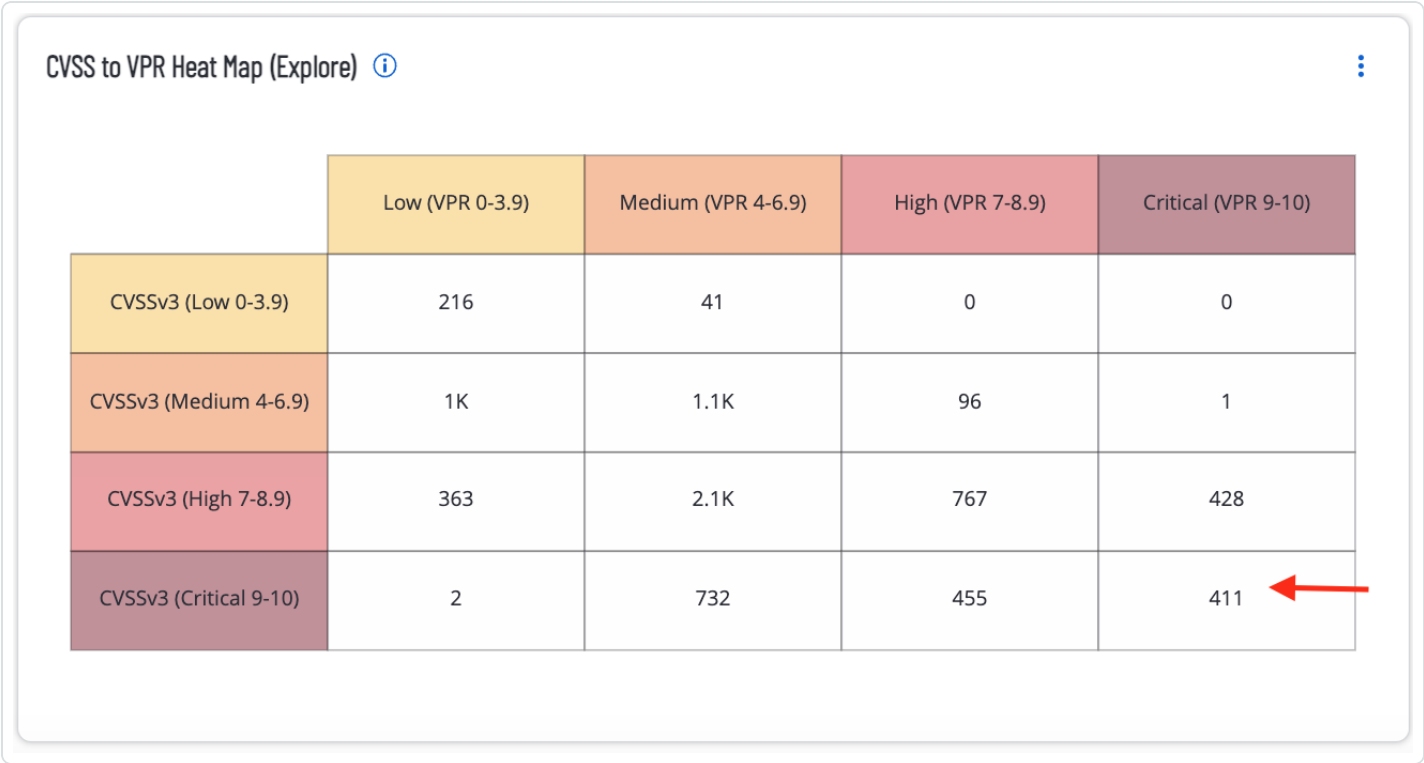
Vulnerabilities by CVSS

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

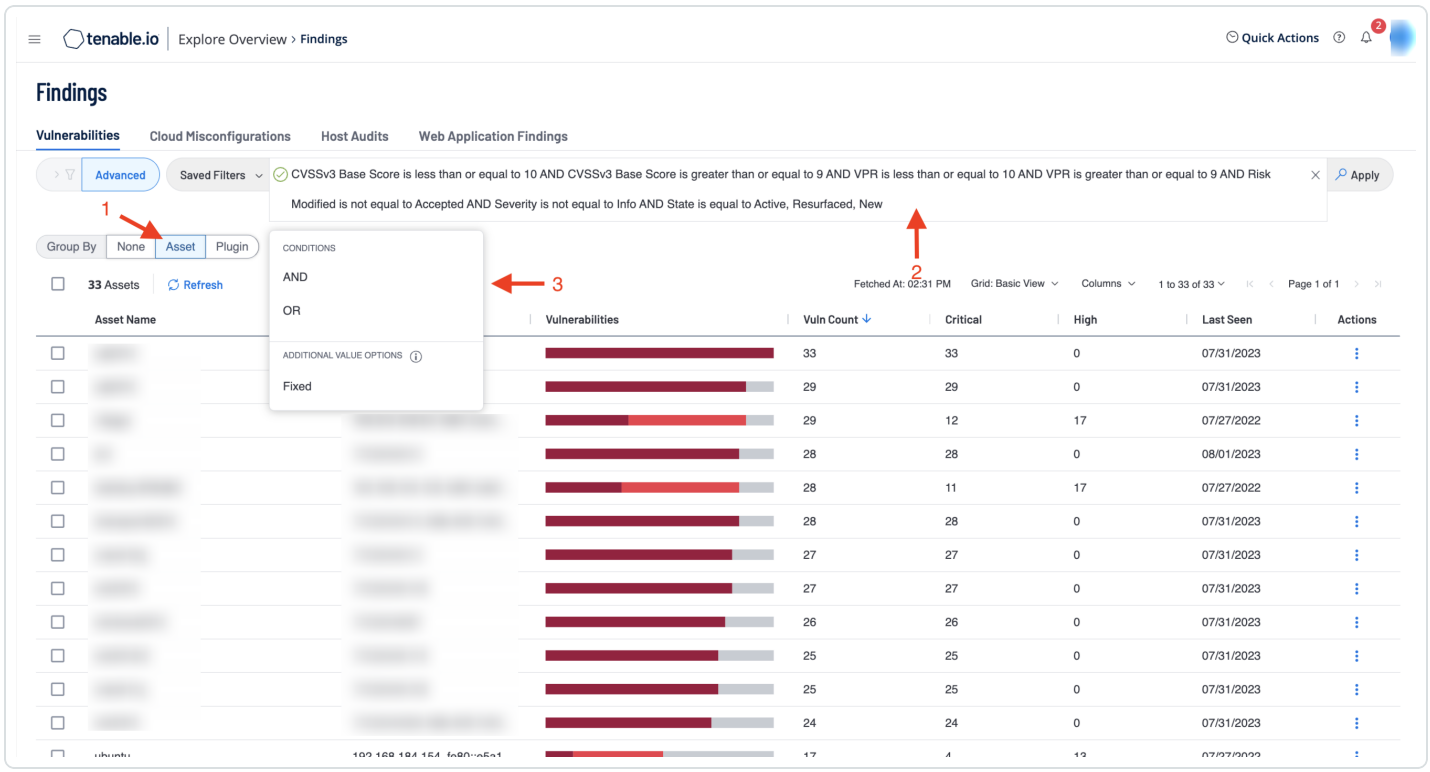
approach, the filters begin in the left upper corner with vulnerabilities that present least risk. Moving to the right and lower down the matrix the colors change darker from yellow to red as the risk levels increase. Click on the cell in the lower right corner of the widget to drill down into details about the most critical CVSSv3 and VPR vulnerabilities.



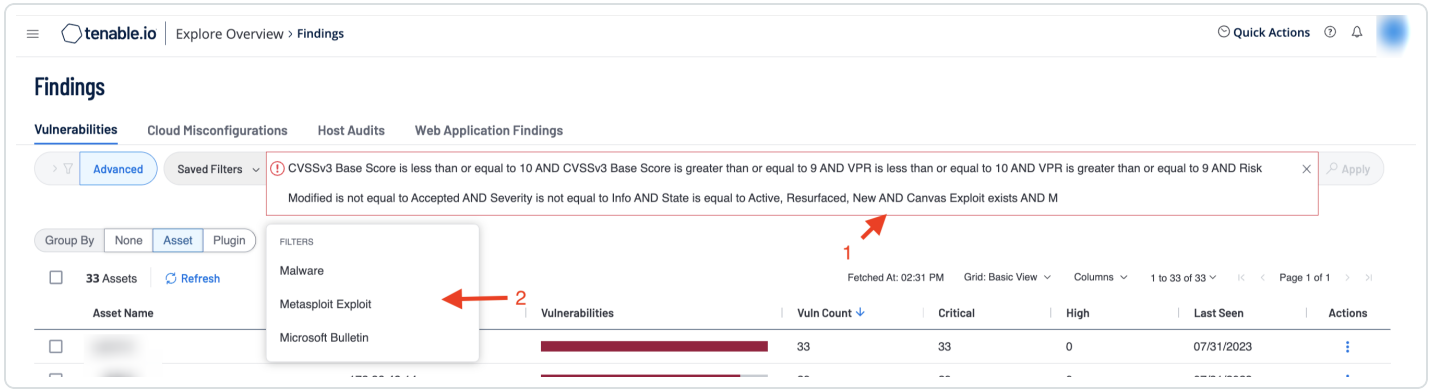
	Low (VPR 0-3.9)	Medium (VPR 4-6.9)	High (VPR 7-8.9)	Critical (VPR 9-10)
CVSSv3 (Low 0-3.9)	216	41	0	0
CVSSv3 (Medium 4-6.9)	1K	1.1K	96	1
CVSSv3 (High 7-8.9)	363	2.1K	767	428
CVSSv3 (Critical 9-10)	2	732	455	411

Drilling Down in Tenable Vulnerability Management

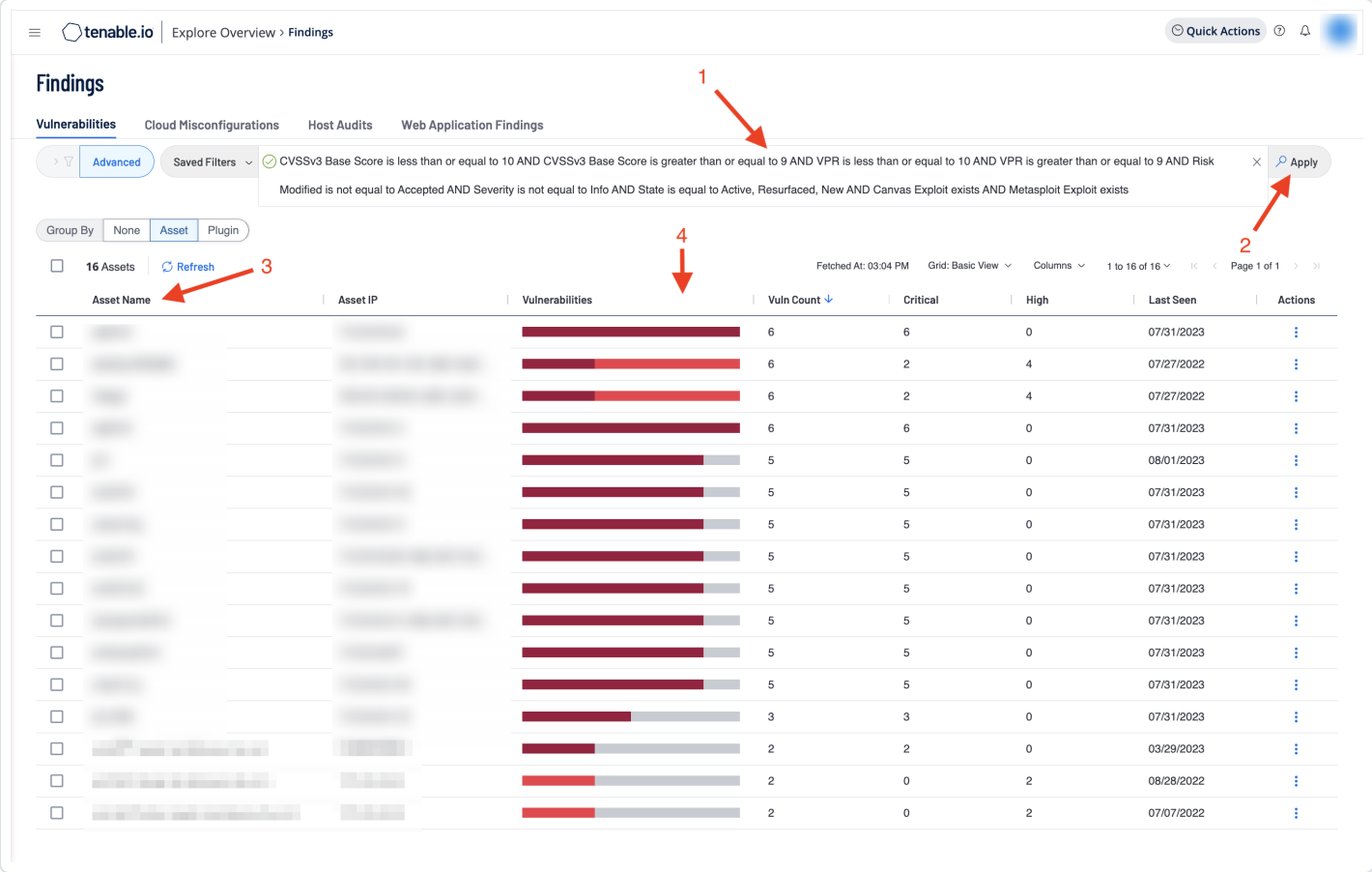
Clicking on any cell displays a Findings page with more details about the vulnerabilities in this category. For this example, the Findings are sorted by **Asset** (**1**). The filter used in the search is displayed in the center conditions field (**2**). Clicking on this field enables users to add additional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



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**."



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.



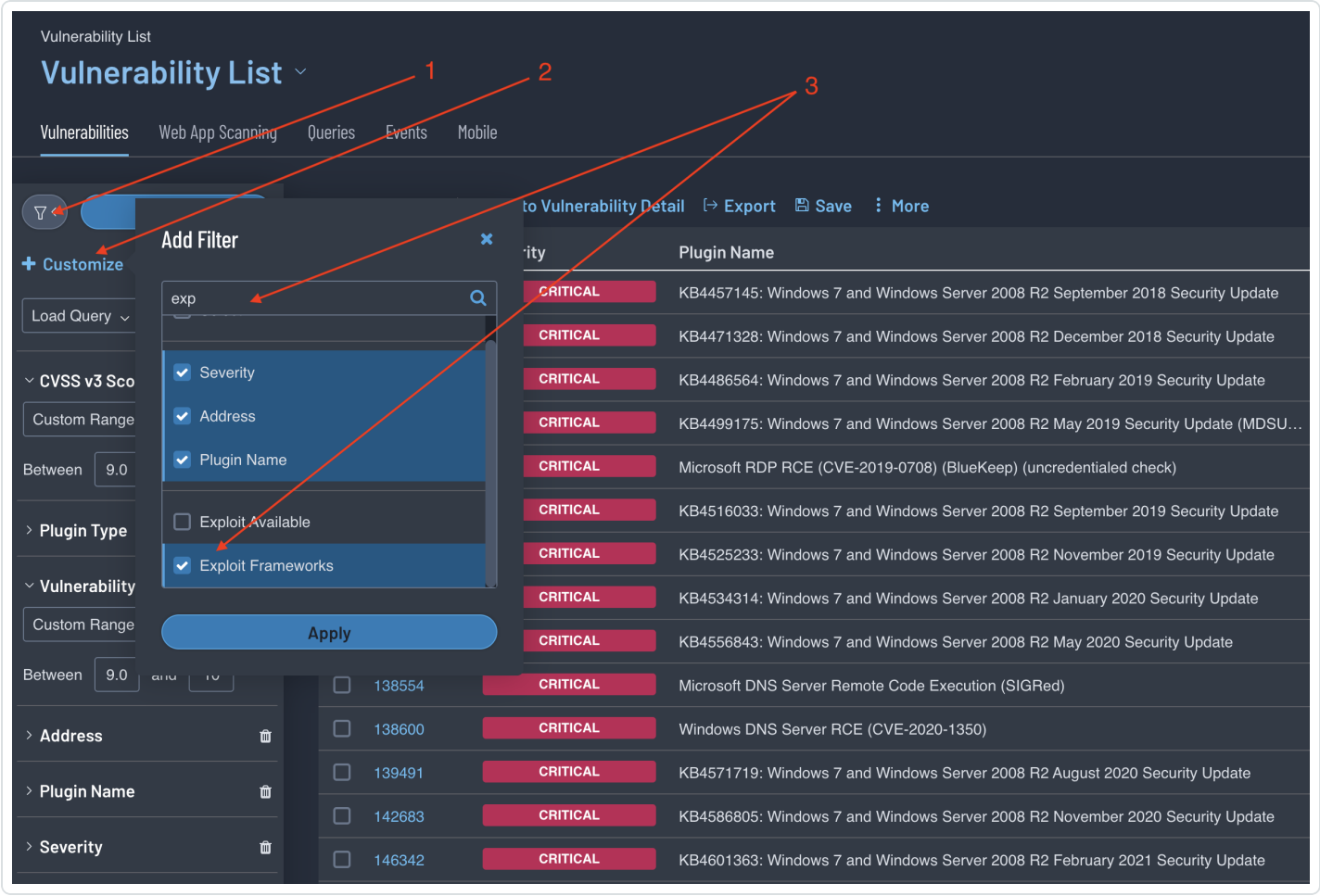
The Tenable Security Center component, as shown below, is similar in layout.

Drilling Down in Tenable Security Center

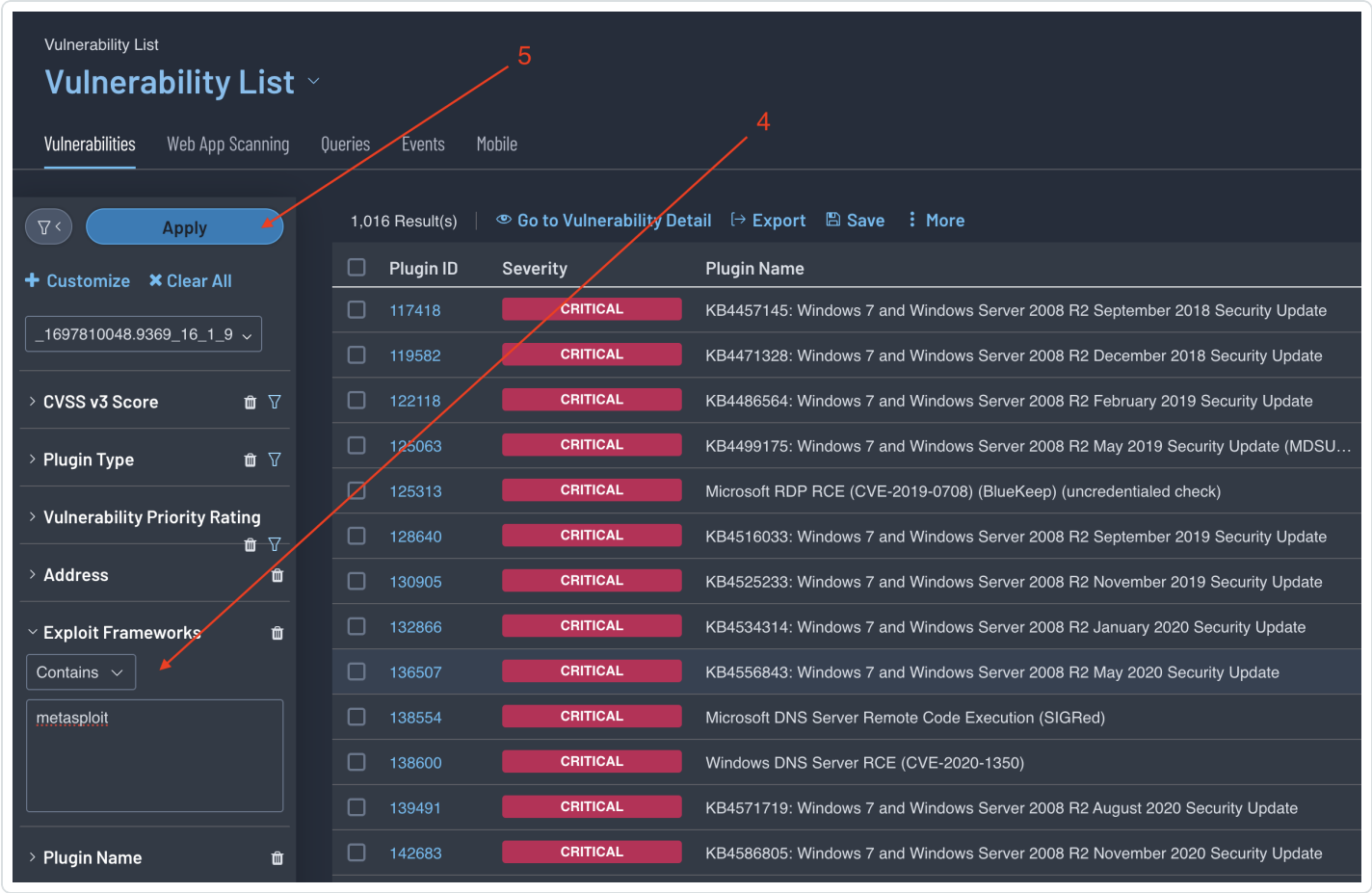
Clicking on any cell displays a Vulnerability Analysis page with more details about the vulnerabilities in this category. For this example, the Vulnerabilities will be sorted by **IP Address (1)**. The filter used

in the search is only displayed in the **Filter** field (**2**). Clicking on this field enables users to add additional Filters.

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**).



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).



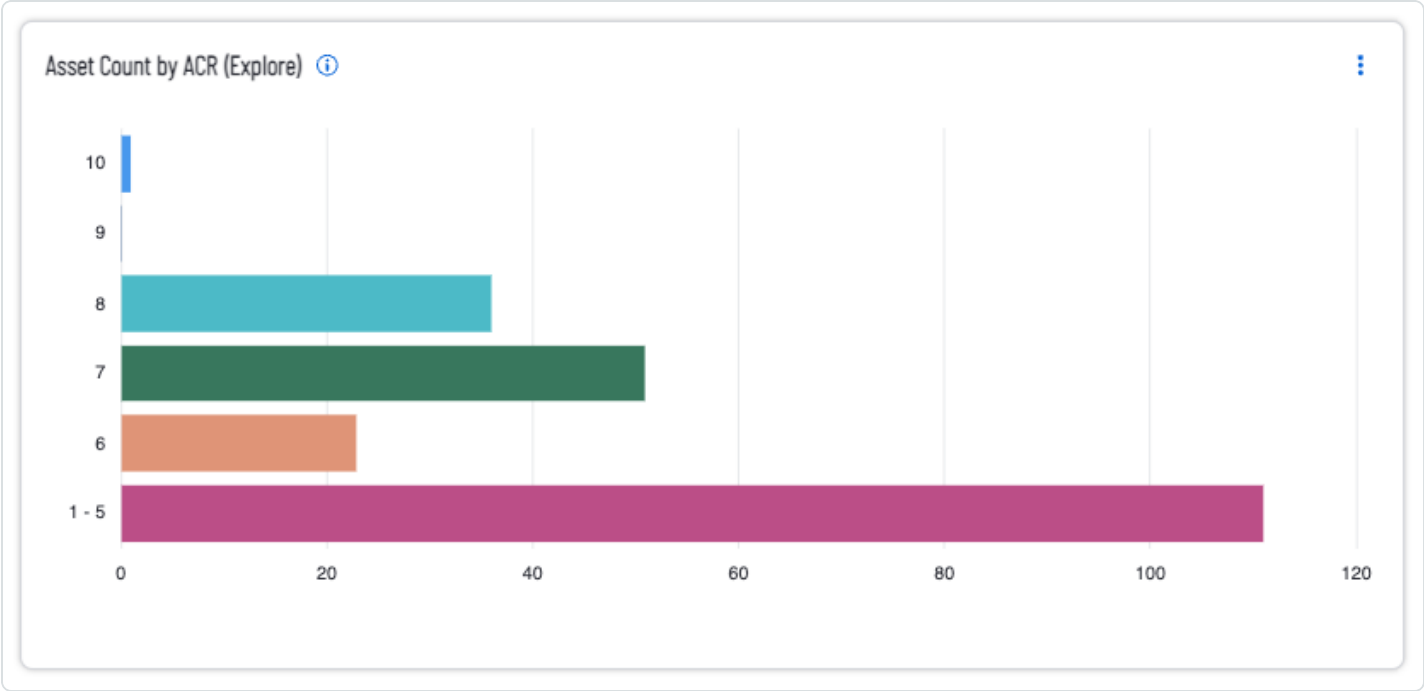
The results that are returned will only include vulnerabilities that include Metasploit in the Exploit Information.

Vulnerabilities by ACR

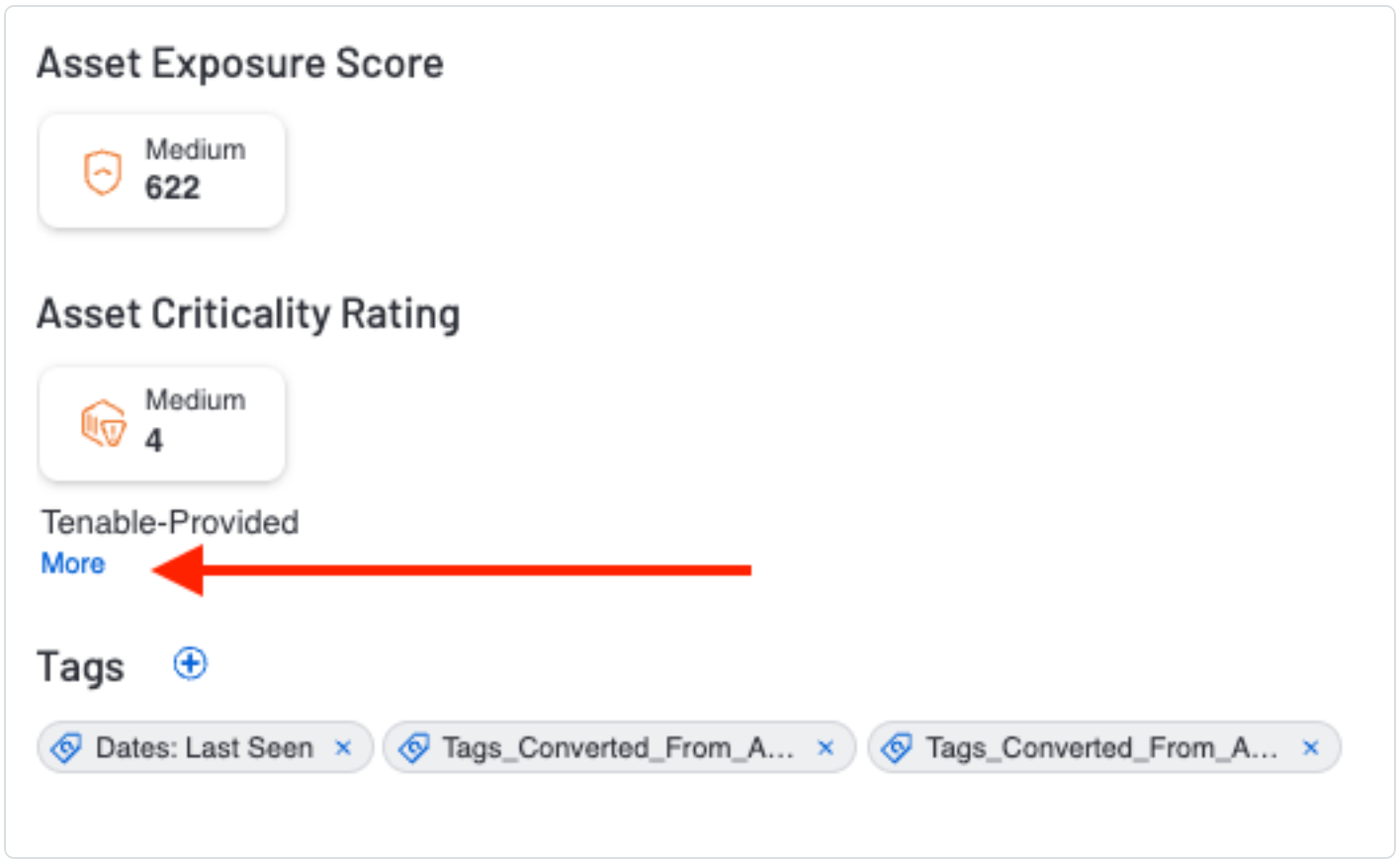
Asset Criticality Rating (ACR) establishes the priority of each asset based on indicators of business value and criticality. ACR is based on several key metrics such as business purpose, asset type, location, connectivity, capabilities, and third-party data. ACRs range from 0 to 10. Assets with a low 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

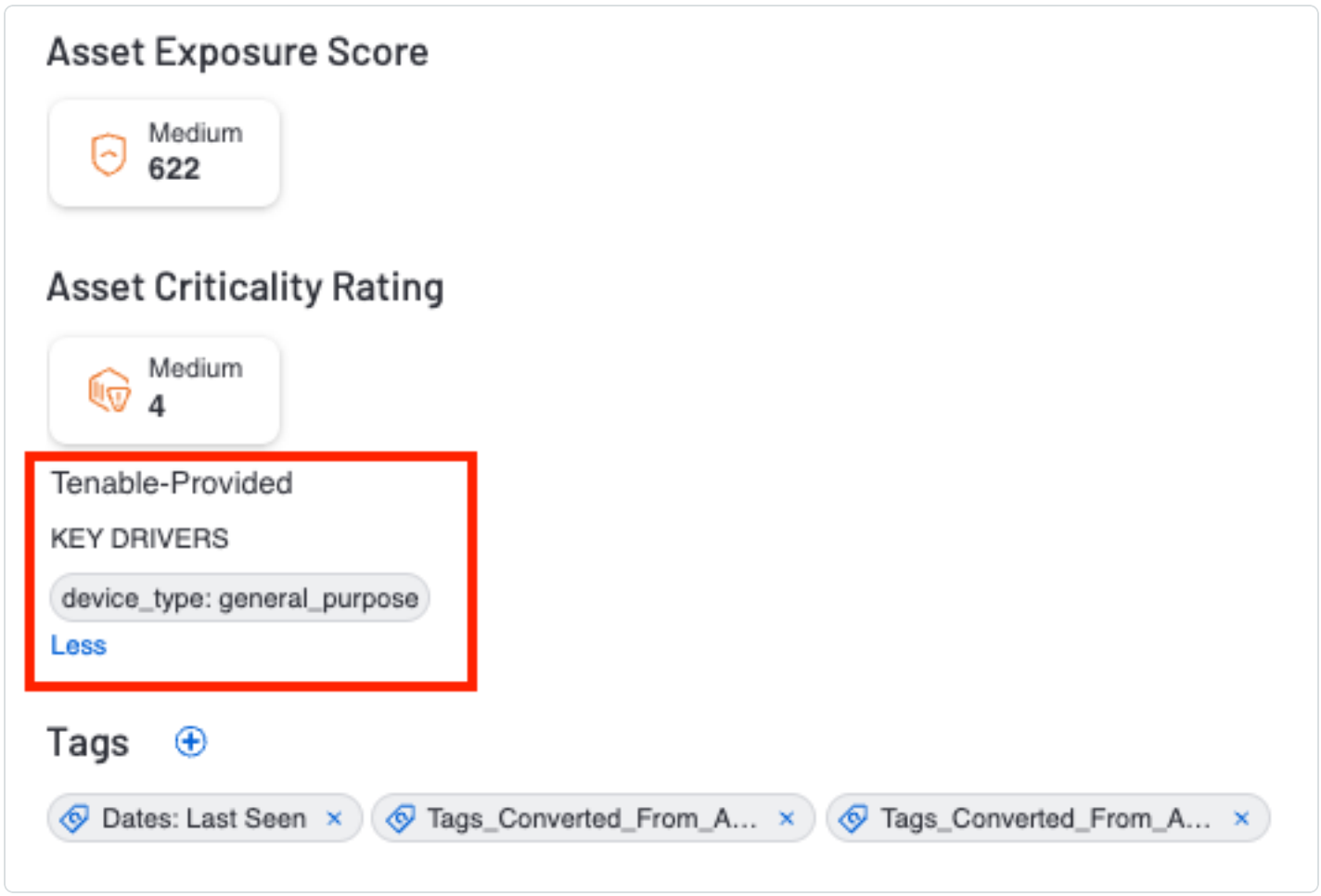
then one bar per score 6 to 10. The requirements for this widget are: Tenable Vulnerability Management, Tenable Web App Scanning, and Tenable Cloud Security.



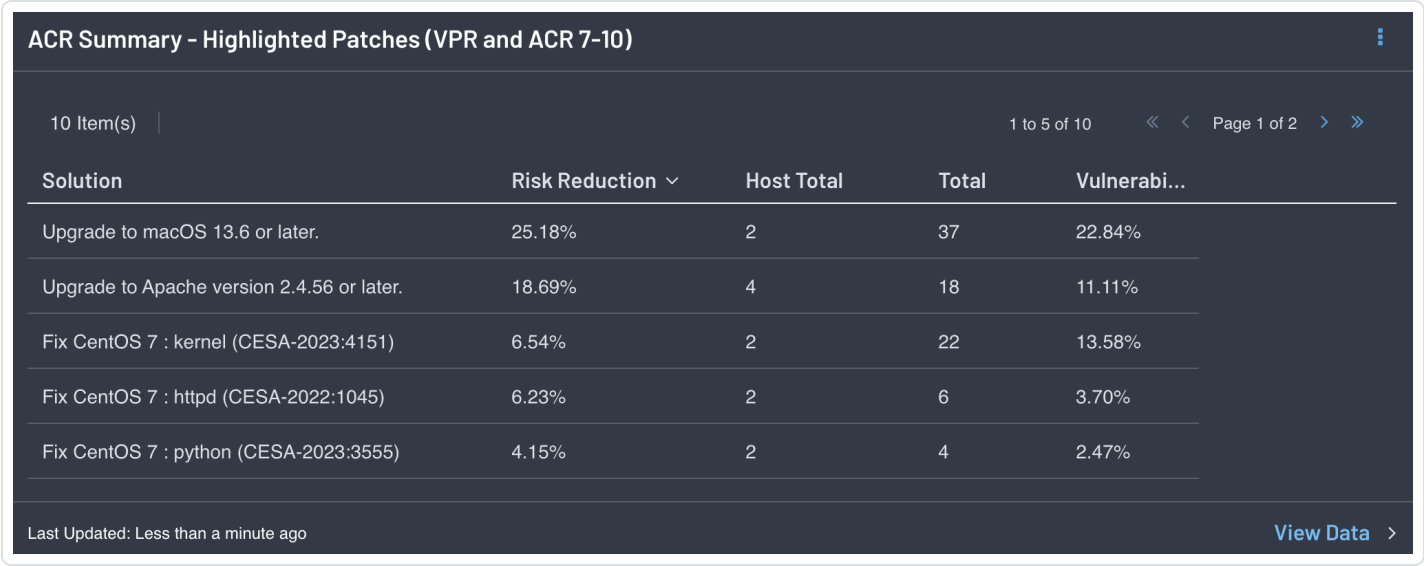
Navigate to the **Assets** page and select an asset to view the asset details and the ACR key driver information for any asset. In the lower left corner of the assets details page reference the **Asset Criticality Rating** information and click **More**.



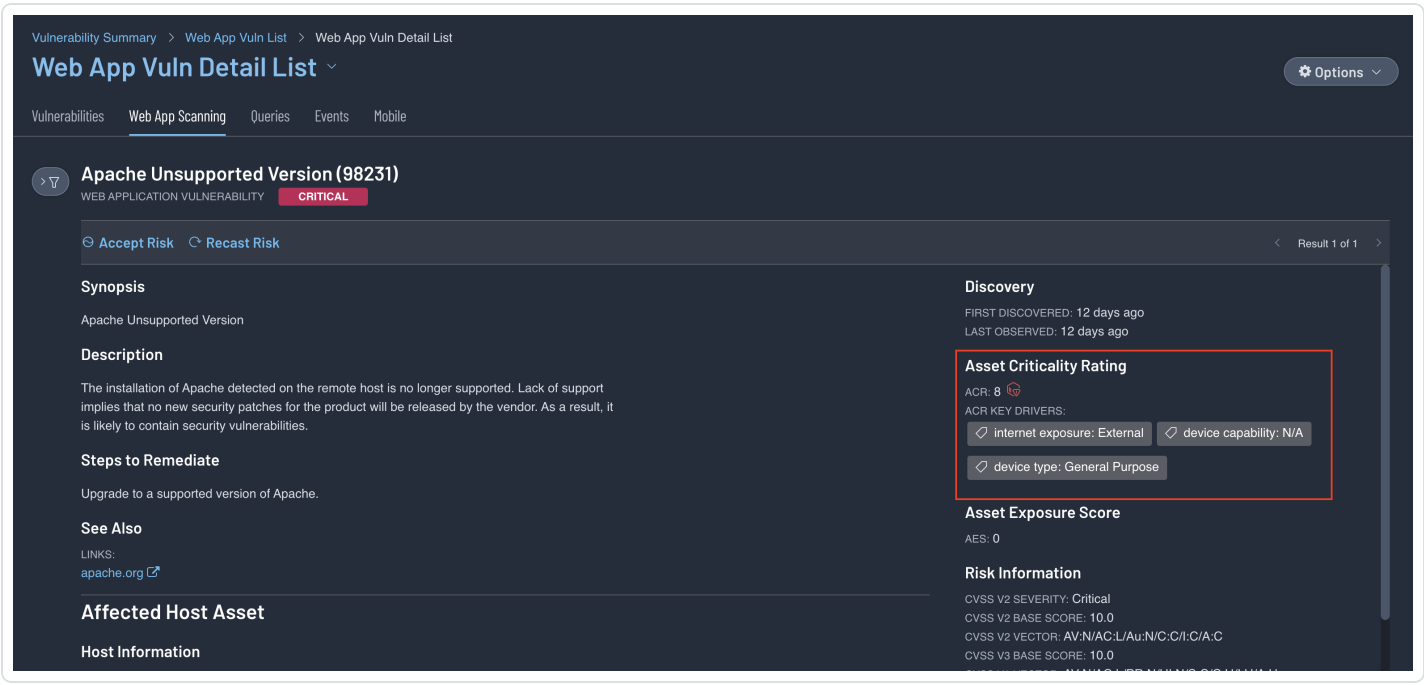
The key drivers are displayed, as shown in the following image:



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



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**.



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.

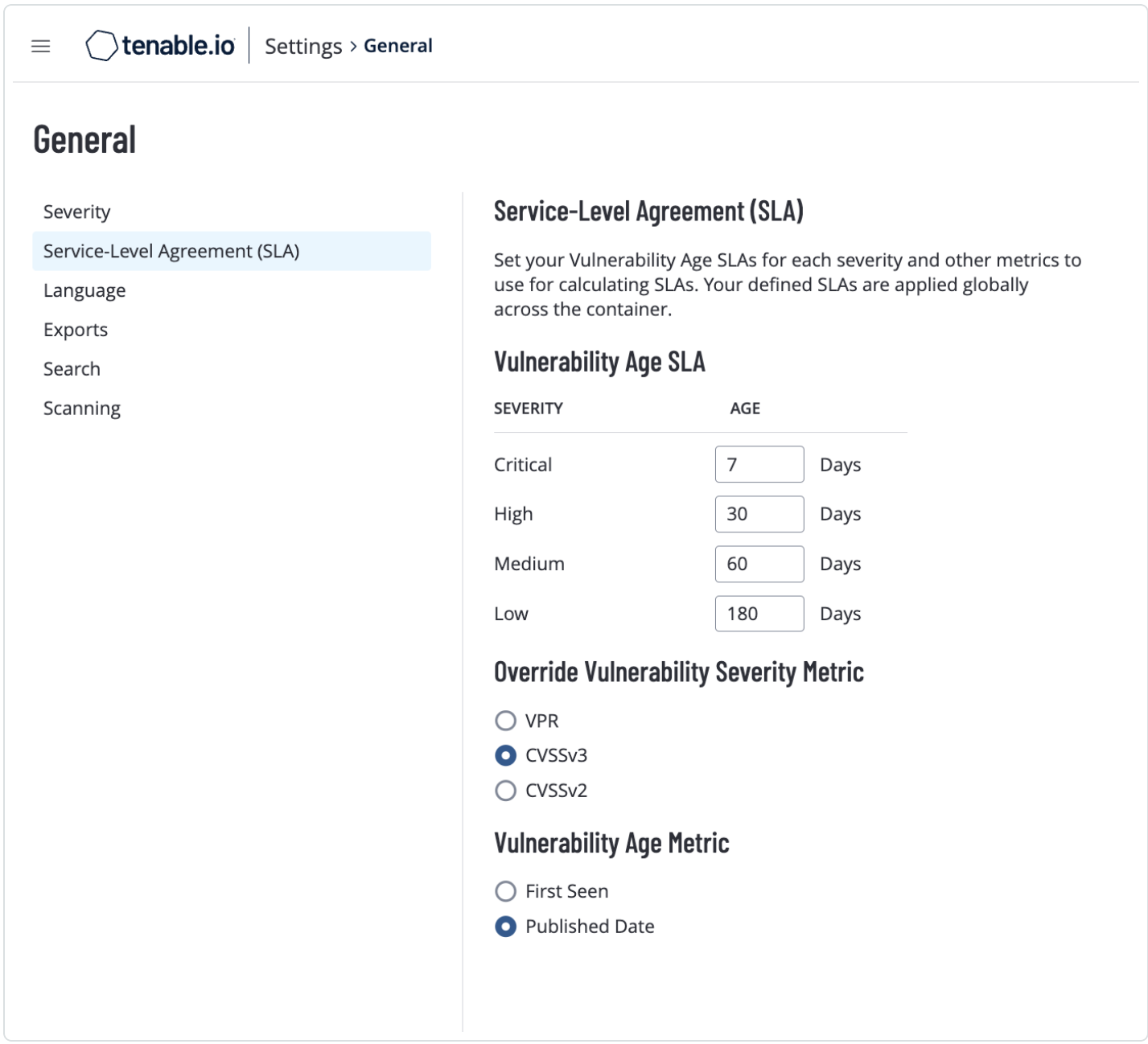
There is no set timetable to resolve vulnerabilities that fits every situation. SLAs can vary from organization to organization, and even vary between business units within the organization. Tenable recommends aligning SLAs with technology or business objectives, starting with the most

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.

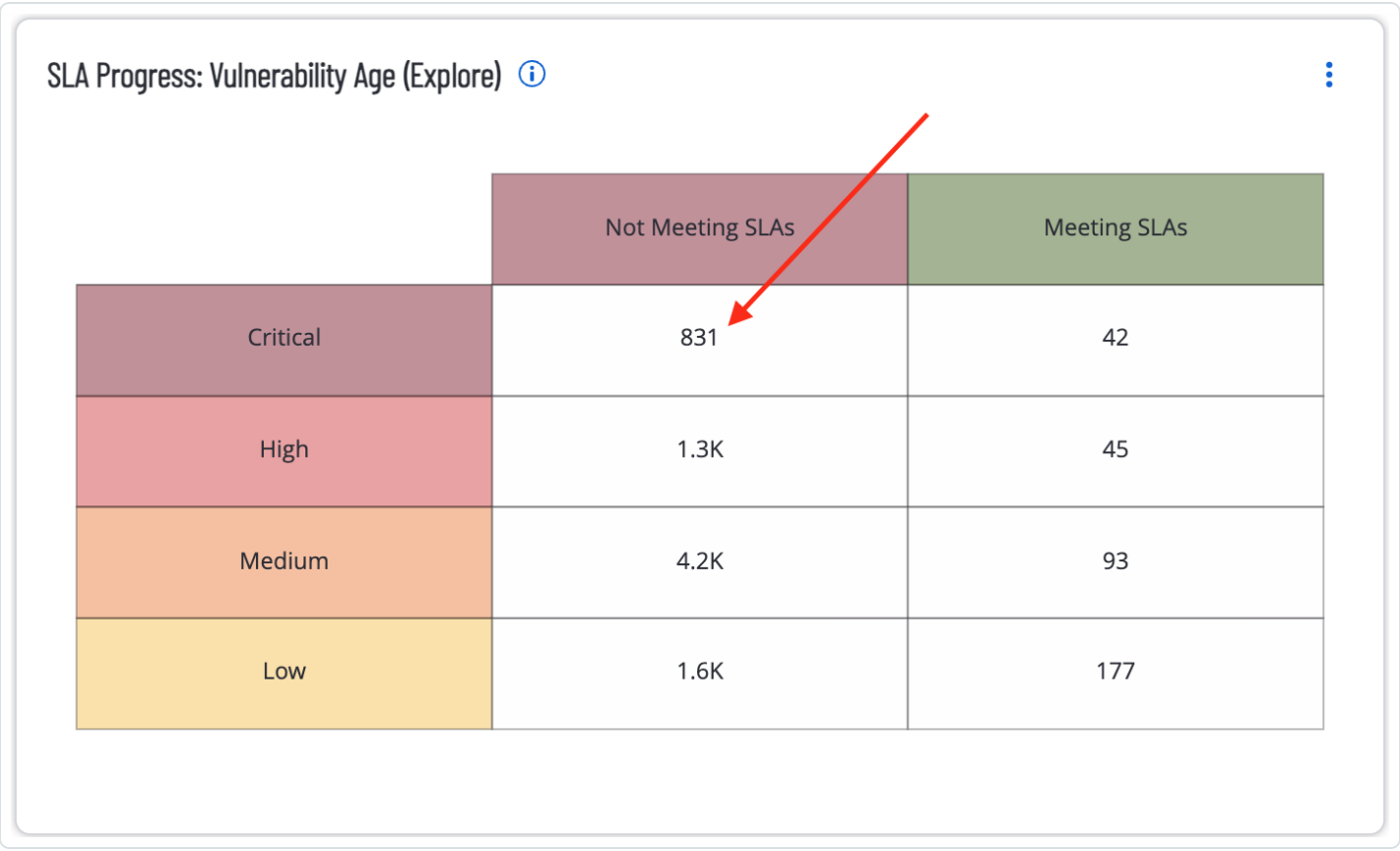
As vulnerabilities are identified, remediation must be prioritized and tracked. Reviewing remediated vulnerabilities and the remediation timeframe provides valuable information to the organization on the effectiveness of the risk remediation program.

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.

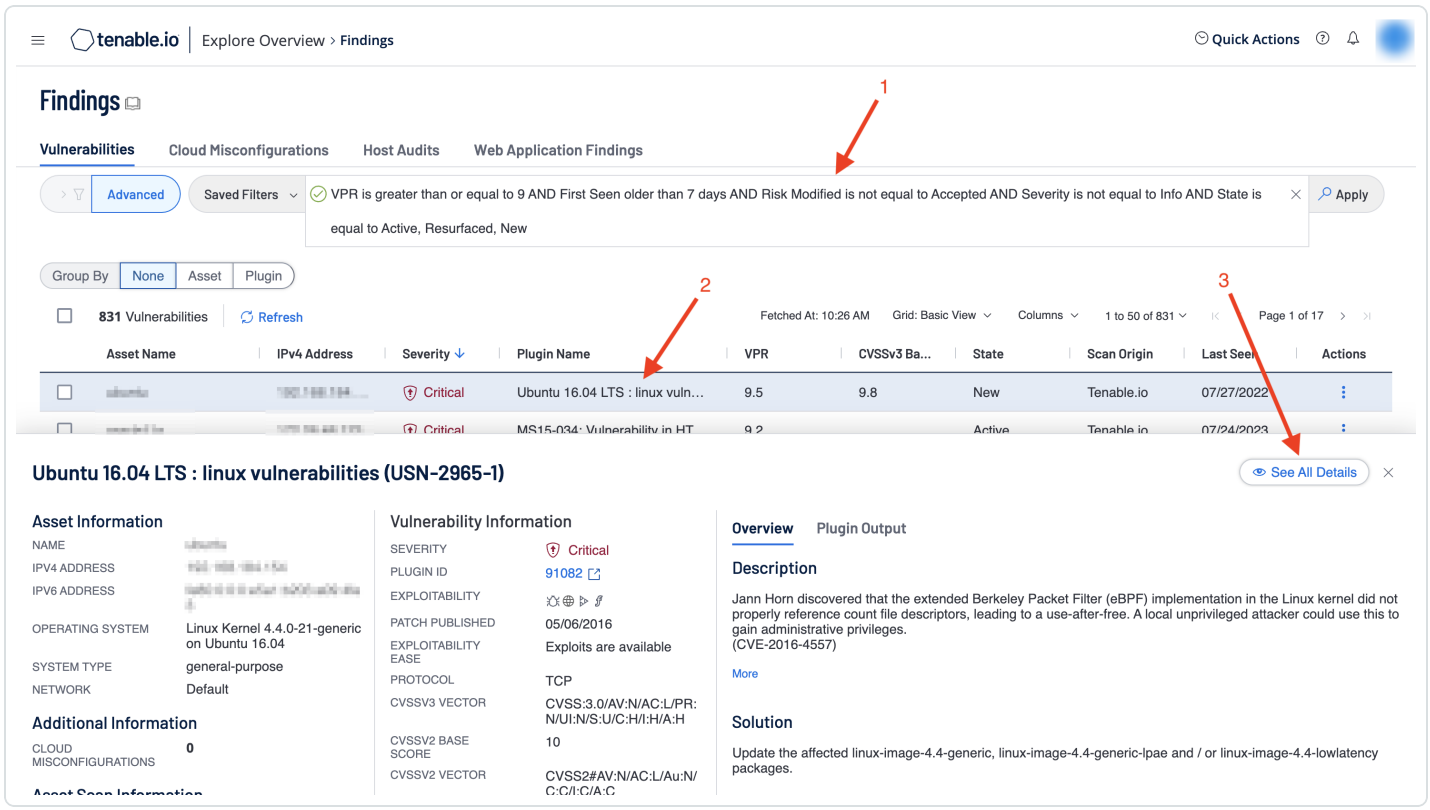


The vulnerabilities that do not meet SLAs are calculated using a date filter for within the last X days. The vulnerabilities that meet SLAs use a date filter for older than X days. When default SLA settings are used, the Critical row displays vulnerabilities with a VPR score greater than 9.0. The High 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.

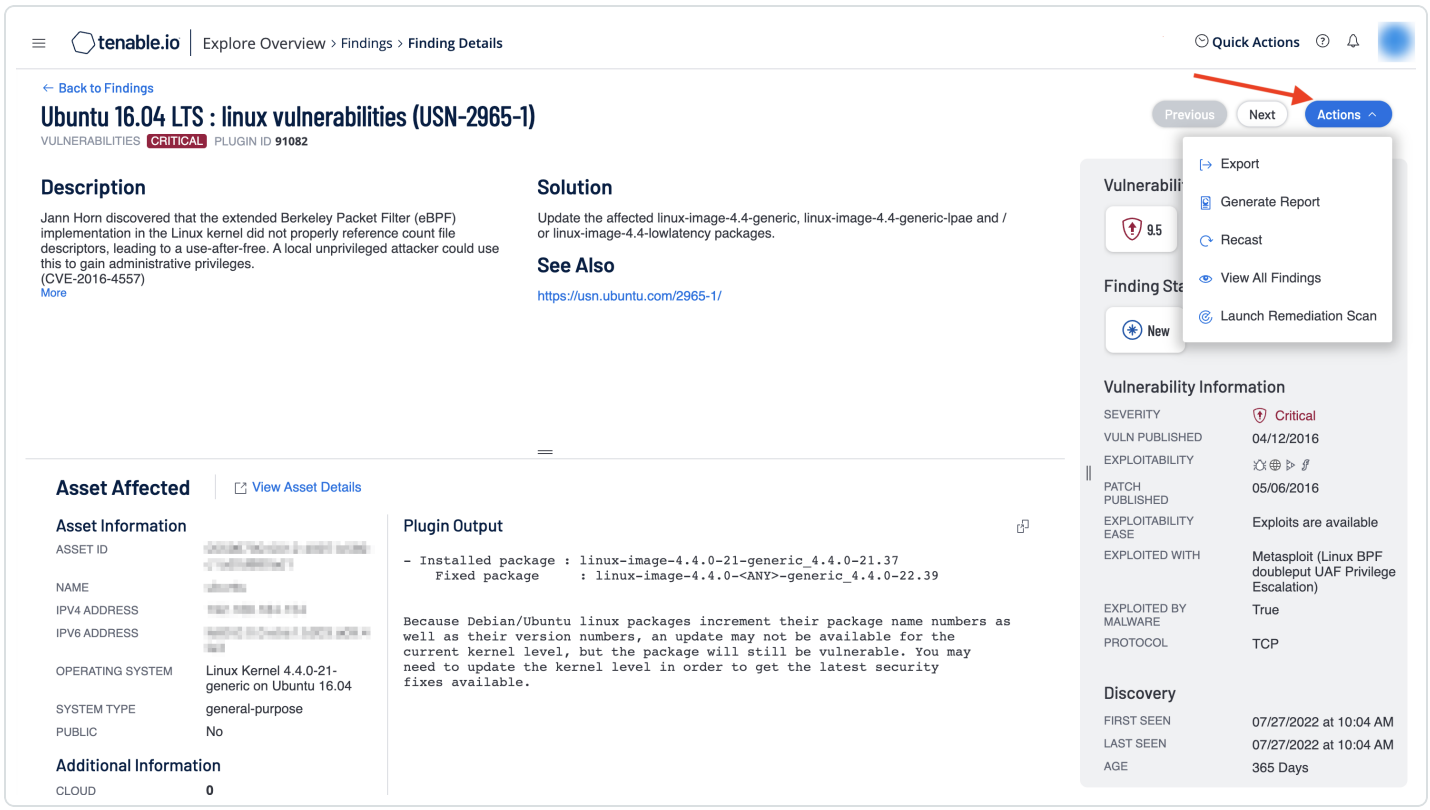


Drilling Down

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



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:



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

Outstanding Remediations

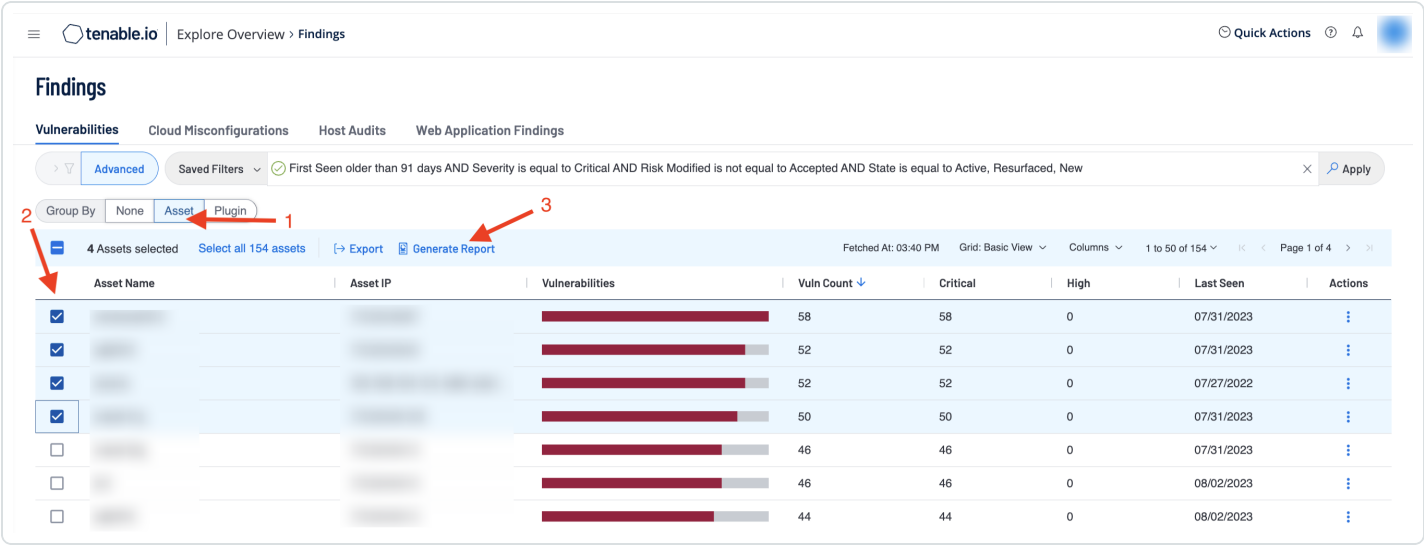
The time between when a vulnerability is discovered and when the vulnerability is typically exploited, or 'time to exploit' is rapidly decreasing. The CISA INSIGHTS report titled Remediate Vulnerabilities for Internet-Accessible Systems notes adversaries, on average, are able to exploit a vulnerability 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.

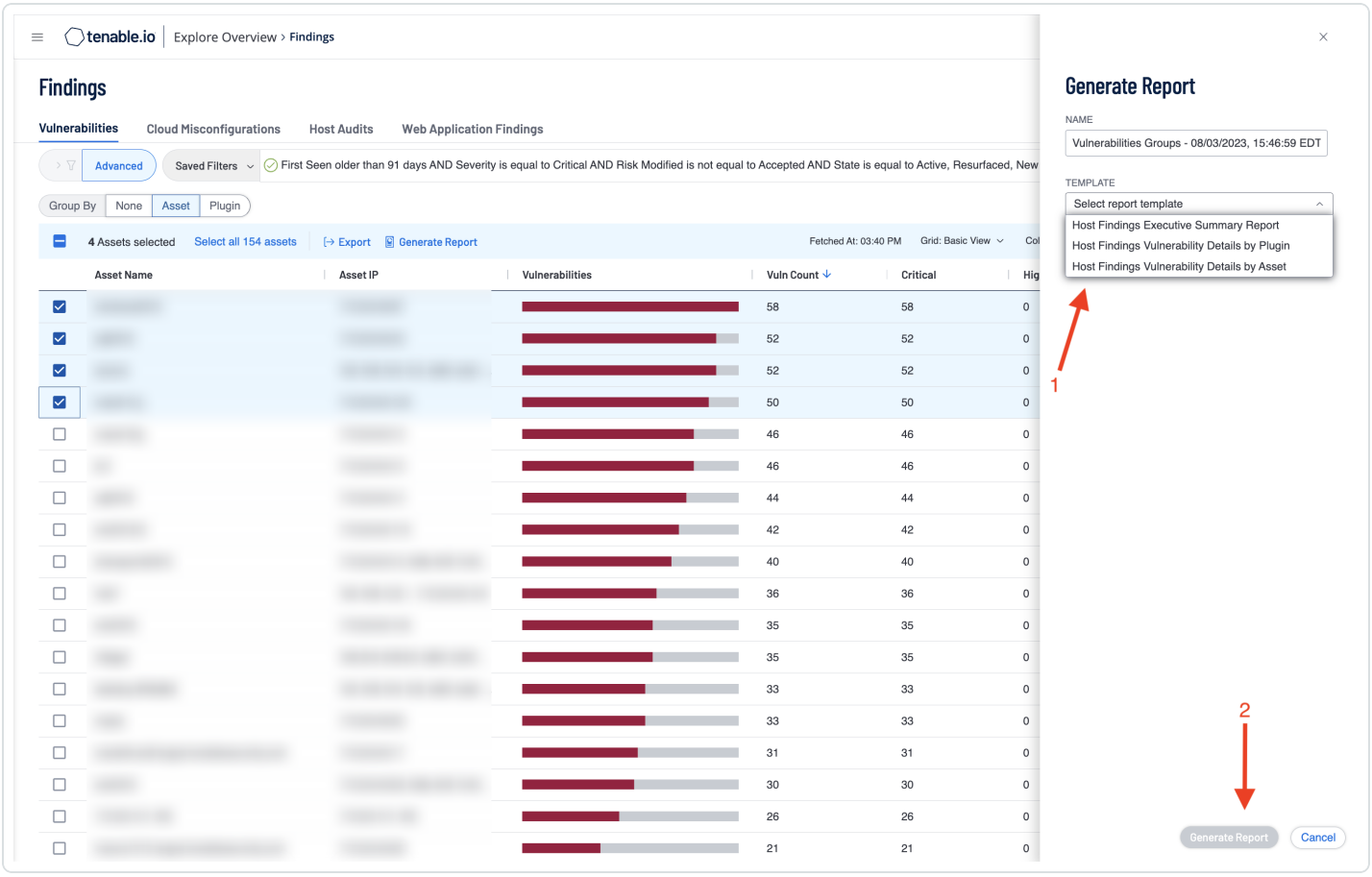
	90+ Days	61-90 Days	31-60 Days	15-30 Days	8-14 Days	0-7 Days
Critical	1.1K	1	18	0	77	4
High	3.8K	1	18	0	31	6
Medium	4.4K	1	37	1	18	4
Low	558	0	1	0	19	0

Drilling Down in Tenable Vulnerability Management

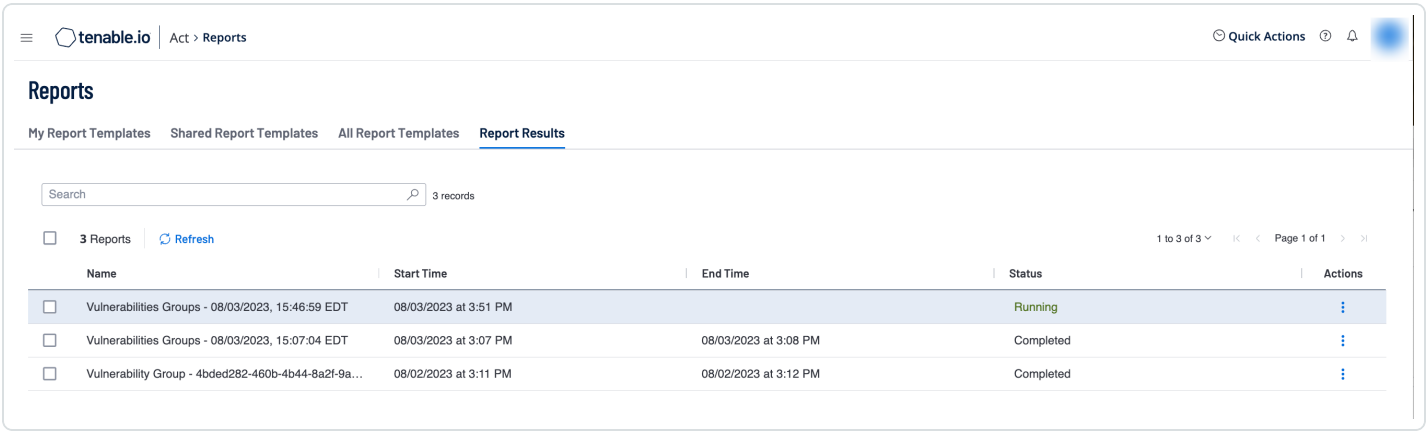
Security analysts can easily generate a report on the assets posing the greatest risk for outstanding remediations by drilling down into the details from this widget. Click on the cell with the most Critical vulnerabilities, which have been outstanding for over 90 days, and select **Asset** (**1**).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



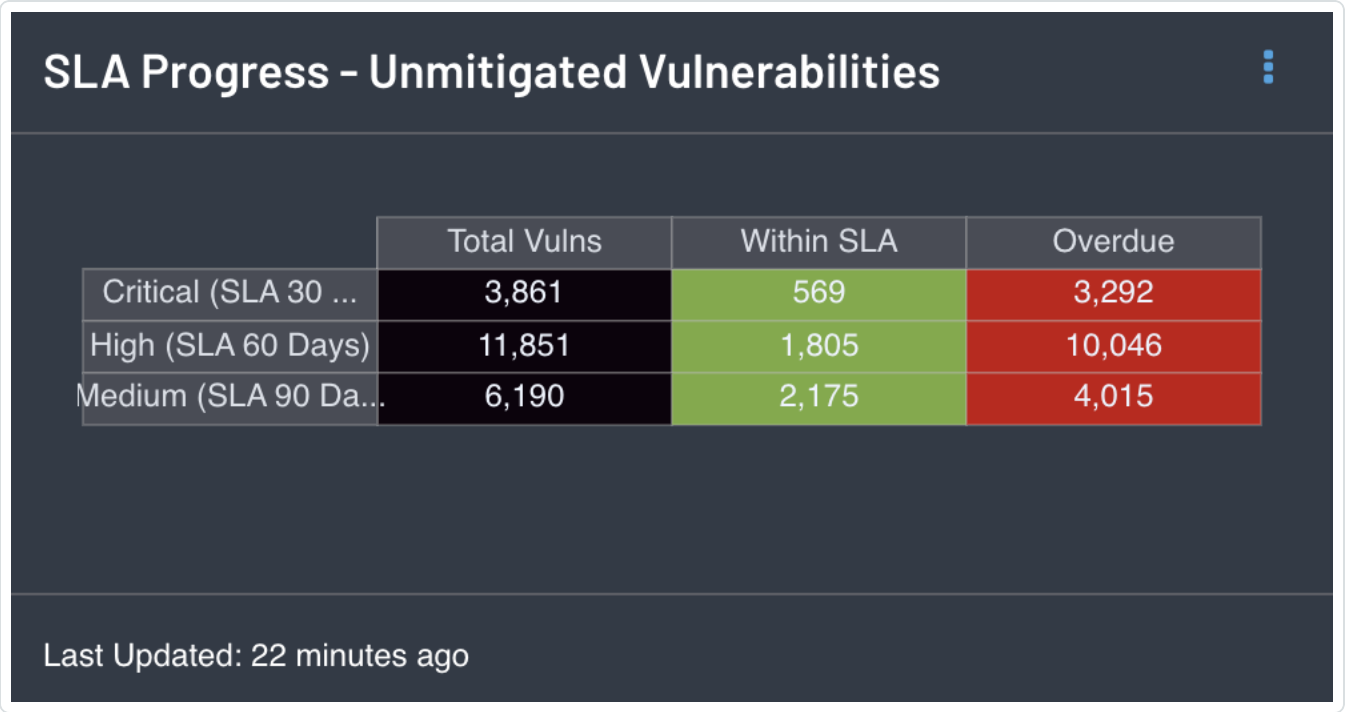
The **Generate Report** window is displayed, where the type of report, such as "**Host Findings Vulnerability Details by Asset**" can be selected (**1**), followed by clicking on the **Generate Report** button (**2**).



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

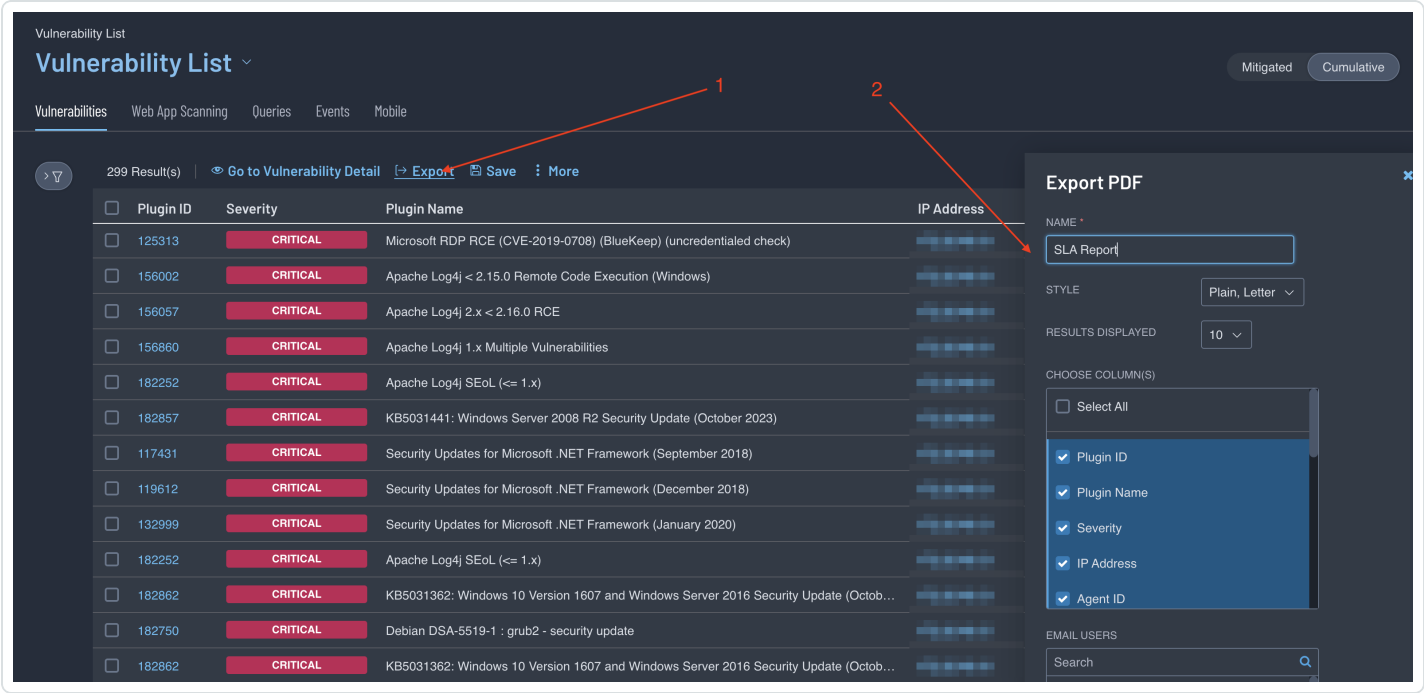


Tenable Security Center does not have a configuration option to define organization specific SLA time-frames. In lieu of that, the **SLA Progress - Unmitigated Vulnerabilities** component provides a summary of vulnerabilities based on the CVSS score and the SLA of 30, 60, 90 days. The best practice is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

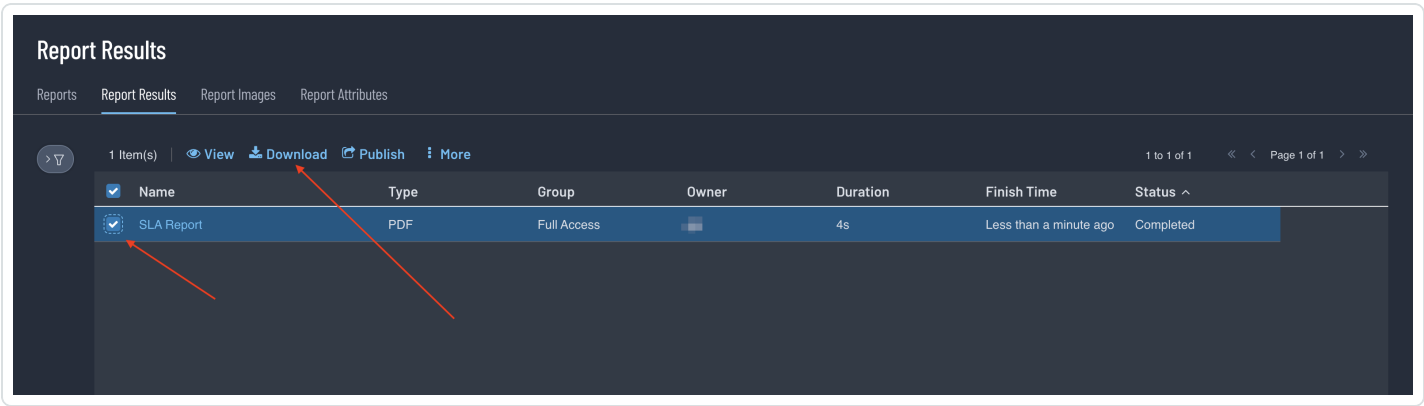


Drilling Down in Tenable Security Center

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.



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.



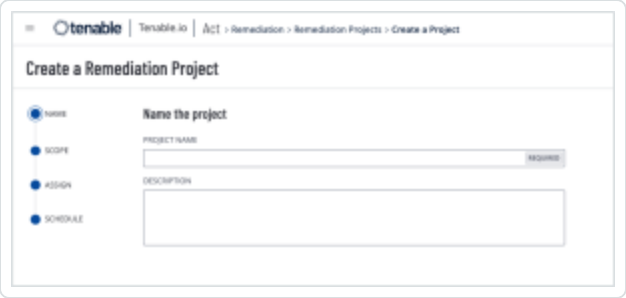
Remediation Summary

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.



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)