Tenable Cyber Exposure Study – Establishing a Software Inventory

Last Revised: July 18, 2025

Table of Contents

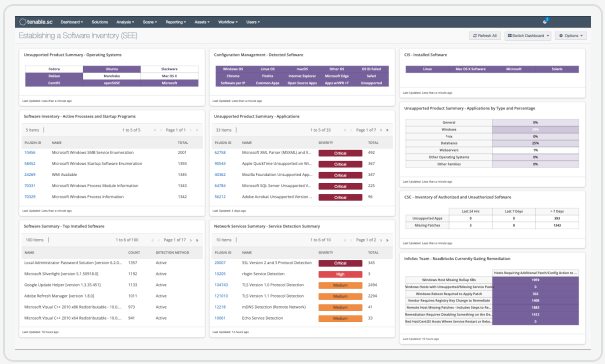
Introduction

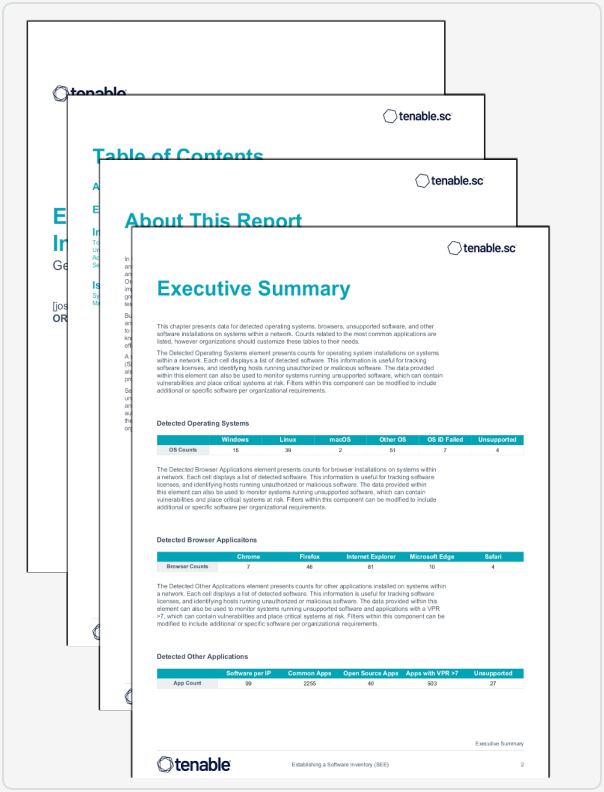
Establishing an inventory of all software and applications running in the environment is a fundamental step in securing your organization. Whether the organization is a small start-up or a global conglomerate, identifying software usage is necessary to ensure software assets are authorized, appropriately licensed, supported, and have the most recent security fixes applied. A software inventory helps demonstrate compliance with regulatory controls and Service Level Agreements (SLA) for software used in the environment. From the perspective of "less is more," a software inventory also identifies unnecessary software running in the environment, which increases the attack surface without providing a business advantage. In fact, running unnecessary software creates overhead and an inefficient run-time environment.

In the event of a security breach, a software inventory is essential to determine what was breached, and who needs to be notified. First responders require a software inventory to perform forensic analysis and determine breach notification requirements for vendors, business partners, and regulatory bodies. Organizations that have a clear understanding of software in their environment can quickly assess a breach impact and identify affected areas. If legal proceedings are involved, an organized software inventory greatly assists in limiting data handed over to Law Enforcement and assists technical staff in depositions or testimony.

Business Continuity and Disaster Recovery plans specify requirements for restoration of critical assets and services, but organizations need to know what these are to establish a Recovery Time Objective (the amount of time to recover a service to an acceptable level of operation) and Recovery Point Objective (the last point of known good data). Developing and maintaining a software inventory is a critical first step in implementing an effective cyber security program. This document provides guidance in using Tenable solutions to gather data and analyze systems to build a software inventory.

Tenable has provided *Establishing Software Inventory (SEE)* Dashboard and Report templates, which are available in the Tenable Security Center feed.





**Queries in this report were limited to 50 for readability purposes.

Benefits of a Software Inventory

From the CISO down to the IT operations staff, all members of an organization's security team need to understand the scope of the organization's digital footprint and have a detailed understanding of what software is authorized. The first step to identify what needs to be protected (and how) is to develop and maintain a software inventory.

Establish Policy

Identifying the software and applications used by the business enables management to establish a criticality rating for the software based on the business application, established through the Business Impact Analysis (BIA) of the Business Continuity Plan (BCP). This information is used to determine the level of protection and breach impact for the confidentiality, integrity, and availability of the data. Management establishes policies and controls for the software that aligns with business and compliance requirements. The software inventory also enables Risk Managers and Vendor Relationship Managers to communicate compliance with internal controls and SLAs for software used in the environment. A software inventory enables the CISO to provide validation of the organization's security program by verifying that software risk has been identified and evaluated.

Establish Procedures

Security operations perform scans to identify operating system and application versions, including unsupported software and unpatched systems. This information is used to establish a secure baseline and measure drift from that baseline. Using Tenable Vulnerability Management or Tenable Security Center, technical staff generate dashboards and reports that can be sent to upper management with a high-level summary of software that is running in the environment. This information determines if the software is authorized, appropriately licensed, supported, and has the most recent security fixes applied.

Developing and Maintaining a Software Inventory

Developing and maintaining a software inventory is a proactive investment in time and resources to gather and analyze information about software assets before a security incident occurs. This process identifies installed software, determines software authorization, groups assets, verifies patches and detects running services. Tenable solutions simplify the task of gathering and analyzing systems to develop and maintain a software inventory.

Identifying Installed Software

Identifying the authorized software assets is an important step to ensure critical assets are protected. The larger the organization, the more difficult the inventory process becomes. Tenable Vulnerability Management and Tenable Security Center help organizations build a software inventory. There are several software discovery plugins that run by default in the following scan templates:

- Basic and Advanced Agent Scans
- Basic and Advanced [Network] Scans
- Credentialed Patch Audit
- Internal PCI Network Scan
- Collect Inventory Agent Scan (see below)

Inventory Agent Scanning in Tenable Vulnerability Management is part of the Frictionless Agent. This new scanning capability leverages Tenable's frictionless assessment capabilities to provide more efficient vulnerability detection, minimizing the Nessus Agent load and installed footprint on the endpoint. Leveraging this new scan policy ensures the agent only runs an inventory collection plugin locally and sends results to Tenable Vulnerability Management for processing in the Frictionless Assessment pipeline. Scan results are presented in the same format as traditional scans. While there is a coverage differential compared to using a traditional agent, the Inventory Agent provides a great option for host-based scanning on hosts with limited resources.

Inventory Agent Scanning is supported on the following platforms:

- Tenable Vulnerability Management Agent scans
- Tenable Security Center imports of Tenable Vulnerability Management cloud agent scans

Note: There is no support for Nessus Manager linked agents.

Performing Authenticated Scans

Authenticated scans are required to enumerate software since software enumerations are considered "Local Checks." More than 120,000 Tenable plugins require successful authentication to occur via a Nessus Agent or a Nessus Scanner before these plugins can run on an asset. These plugins are of the plugin type "Local" rather than "Remote." The Tenable Plugins page allows you to search for Local Plugins and Remote Plugins to determine which plugins require successful authentication.

Note: *Plugin Type* in Tenable Security Center refers to whether a plugin is in the category of **Active** (Nessus), **Passive** (Nessus Network Monitor), or **Compliance** (Audit File scan results). *Plugin Type* in Tenable Vulnerability Management and on the Tenable Plugins Page refers to whether a plugin is **Local**, **Remote**, or **Combined**. Combined refers to plugins that will run in both authenticated and unauthenticated scans. These plugins will run and generate plugin output regardless of successful authentication. Plugins that fall into an Operating System Plugin Family, such as VMware ESX Local Security Checks, are considered "Local Checks" and require authentication to run. Although most of the Local Security Checks plugin families contain the words "Local Security Checks," there are other plugin families that require successful authentication to run, such as the Windows : Microsoft Bulletins plugin family. Verification that scans complete with successful or expected levels of authentication is essential to determine if scans are successful to avoid false negatives. Check the Learn More section of this document for more information about authenticated scans and plugin types.

Nessus scanners used with Tenable Vulnerability Management and Tenable Security Center support the use of credentials to log in to a system to provide information about configuration settings that would not be visible from the network. For example, a credentialed scan can get information about the type of hardware that is running. Hardware drivers have life cycles just like any other type of software, and are subject to the same security issues. The Center for Internet Security (CIS) provides consensus benchmarks that set security hardening standards. A credentialed scan can verify that systems are configured in accordance with a known "gold standard."

The most common software enumeration plugins are OS Identification (11936), Microsoft Windows Installed Software Enumeration (credentialed check) (20811), Software Enumeration (SSH) (22869), and List Installed Mac OS X Software (83991). There are several other software enumeration plugins that provide information that can help build a software inventory:

- OS Fingerprinting via DHCP (7120)
- Oracle Installed Software Enumeration (Linux / Unix) (71642)
- Oracle Installed Software Enumeration (Windows) (71643)
- OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library) (97993)
- Unix Software Discovery Command Checks (152741)
- Unix Software Discovery Commands Available (152742)
- Unix Software Discovery Commands Not Available (152743)

> **Plugin Spotlight**: Plugin ID 22869, Software Enumeration (SSH), identifies the package list on Linux systems, which includes package name, version, epoch information for each package installed on the system, and (on RPM-based systems) the date the operating system reports that a package was installed. This information is included in the plugin output (also referred to as "vulnerability text") in the scan results.

The package installation date may not be displayed in the scan results for some systems, such as Debian.

Tenable products will attempt to store a version of the package list that includes dates separately for all Tenable-supported Linux operating systems running RPM-based packaging. If available, the package installation date will be displayed in the "Software Enumeration (SSH)" plugin, 22869.

The following is a sample of the Plugin Output for Plugin 22869:

```
Here is the list of packages installed on the remote CentOS Linux system :

  setup-2.8.14-20.el6_4.1|(none)      Wed Feb 19 04:17:22 2014
  basesystem-10.0-4.el6|(none)      Wed Feb 19 04:17:22 2014
  kernel-firmware-2.6.32-431.el6|(none)      Wed Feb 19 04:17:24 2014
  nss-softokn-freebl-3.14.3-9.el6|(none)      Wed Feb 19 04:17:26 2014
  glibc-2.12-1.132.el6|(none)      Wed Feb 19 04:17:33 2014
  bash-4.1.2-15.el6_4|(none)      Wed Feb 19 04:17:34 2014
  libcap-2.16-5.5.el6|(none)      Wed Feb 19 04:17:34 2014
  info-4.13a-8.el6|(none)      Wed Feb 19 04:17:34 2014
  chkconfig-1.3.49.3-2.el6_4.1|(none)      Wed Feb 19 04:17:35 2014
  libcom_err-1.41.12-18.el6|(none)      Wed Feb 19 04:17:35 2014
  db4-4.7.25-18.el6_4|(none)      Wed Feb 19 04:17:35 2014
  nss-util-3.15.1-3.el6|(none)      Wed Feb 19 04:17:35 2014
  libsepol-2.0.41-4.el6|(none)      Wed Feb 19 04:17:36 2014
  sed-4.2.1-10.el6|(none)      Wed Feb 19 04:17:36 2014
  bzip2-libs-1.0.5-7.el6_0|(none)      Wed Feb 19 04:17:37 2014
  libstdc++-4.4.7-4.el6|(none)      Wed Feb 19 04:17:37 2014
  gawk-3.1.7-10.el6|(none)      Wed Feb 19 04:17:37 2014
  libgpg-error-1.7-4.el6|(none)      Wed Feb 19 04:17:38 2014
  libudev-147-2.51.el6|(none)      Wed Feb 19 04:17:38 2014
  grep-2.6.3-4.el6|(none)      Wed Feb 19 04:17:38 2014
  sqlite-3.6.20-1.el6|(none)      Wed Feb 19 04:17:39 2014
  libidn-1.18-2.el6|(none)      Wed Feb 19 04:17:39 2014
  xz-libs-4.999.9-0.3.beta.20091007git.el6|(none)      Wed Feb 19 04:17:39 2014
  libgcrypt-1.4.5-11.el6_4|(none)      Wed Feb 19 04:17:39 2014
  findutils-4.4.2-6.el6|1      Wed Feb 19 04:17:40 2014
  checkpolicy-2.0.22-1.el6|(none)      Wed Feb 19 04:17:40 2014
  which-2.19-6.el6|(none)      Wed Feb 19 04:17:40 2014
  pth-2.0.7-9.3.el6|(none)      Wed Feb 19 04:17:41 2014
  sysvinit-tools-2.87-5.dsf.el6|(none)      Wed Feb 19 04:17:41 2014
  p11-kit-0.18.5-2.el6|(none)      Wed Feb 19 04:17:41 2014
  ca-certificates-2013.1.94-65.0.el6|(none)      Wed Feb 19 04:17:42 2014
  nss-softokn-3.14.3-9.el6|(none)      Wed Feb 19 04:17:43 2014
  upstart-0.6.5-12.el6_4.1|(none)      Wed Feb 19 04:17:44 2014
```

Common searches for Tenable software enumeration plugins and plugin results include:

- *Plugin Name* **contains** enumeration
- *Plugin Name* **contains** discovery

- *Plugin Name* **contains** list installed
- *Plugin Name* **contains** installed software
- *Plugin ID* **equals** 11936, 20811, 22869, 83991, 97993, 152741, 71642, 71643, 152742, 152743, 7120

The following is a sample of the Plugin Output from Plugin 20811:

Plugin Output

```
The following software are installed on the remote host :

Microsoft Edge  [version 101.0.1210.39]  [installed on 2022/05/06]
Microsoft Edge Update  [version 1.3.161.35]
Microsoft Edge WebView2 Runtime  [version 101.0.1210.32]  [installed on 2022/05/01]
Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.29.30133  [version 14.29.30133.0]
Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.29.30133  [version 14.29.30133.0]
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.29.30133  [version 14.29.30133]  [installed on 2022/03/13]
Microsoft Update Health Tools  [version 4.67.0.0]  [installed on 2022/04/04]
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.29.30133  [version 14.29.30133]  [installed on 2022/03/13]
Nessus Agent (x64)  [version 10.1.3.20118]  [installed on 2022/04/05]
VMware Tools  [version 12.0.0.19345655]  [installed on 2022/03/13]
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.30133  [version 14.29.30133]  [installed on 2022/03/13]
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.29.30133  [version 14.29.30133]  [installed on 2022/03/13]
```

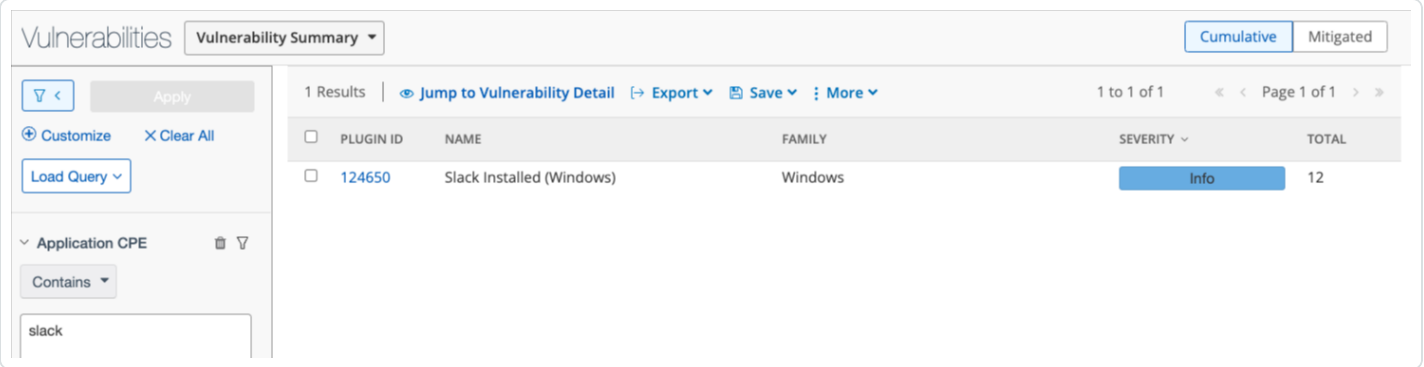
The following image displays the results of the software enumeration plugin for macOS, Plugin ID 83991:

```
System Profiler managed applications:

50onPaletteServer [version 1.1.0]
  Location: /System/Library/Input Methods/50onPaletteServer.app

ABAssistantService [version 11.0]
  Location:
/System/Library/Frameworks/AddressBook.framework/Versions/A/Helpers/ABAssistantS
ervice.app

About This Mac [version 1.0]
  Location: /System/Library/CoreServices/Applications/About This Mac.app

AccessibilityVisualsAgent [version 1.0]
  Location:
/System/Library/PrivateFrameworks/AccessibilitySupport.framework/Versions/A/Reso
urces/AccessibilityVisualsAgent.app

Activity Monitor [version 10.14]
  Location: /System/Applications/Utilities/Activity Monitor.app

Add Printer [version 17]
  Location: /System/Library/CoreServices/AddPrinter.app

AddressBookManager [version 11.0]
  Location:
/System/Library/Frameworks/AddressBook.framework/Versions/A/Helpers/AddressBookM
anager.app

AddressBookSourceSync [version 11.0]
  Location:
/System/Library/Frameworks/AddressBook.framework/Versions/A/Helpers/AddressBookS
ourceSync.app
```

Determining Software Authorization and Support

Once software is enumerated, there are additional plugins that can help determine how many instances of each version of software are running in the environment. This data helps determine

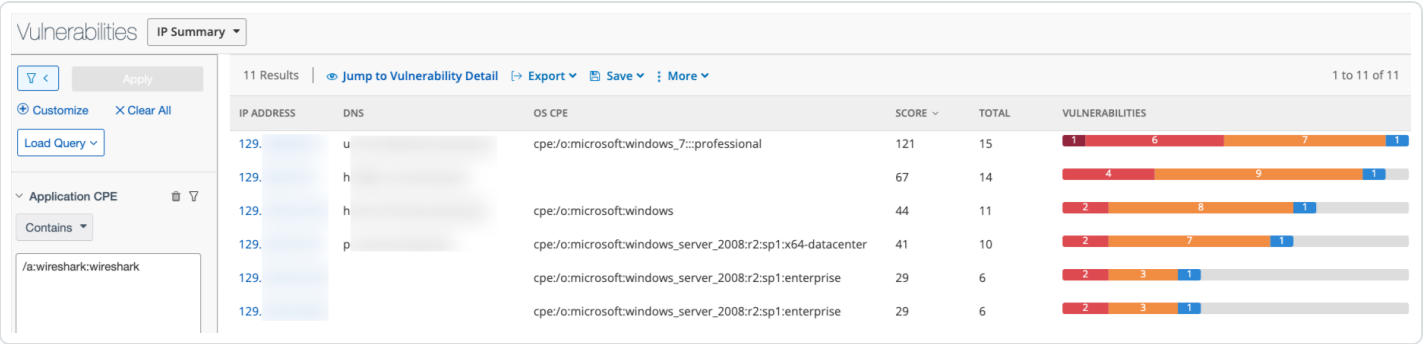
software authorization and support. Tenable plugins can enumerate unsupported operating systems, databases, web servers, browsers, and other software. FINRA Rules forbid financial institutions from using any digital communication applications that cannot preserve records of business-related communications, such as WhatsApp, Signal, or Telegram. Tenable plugins can be used to detect these applications, saving the organization from large fines levied by the Securities and Exchange Commission (SEC). The following is a sample search using CPE to find a commonly used chat and collaboration application.



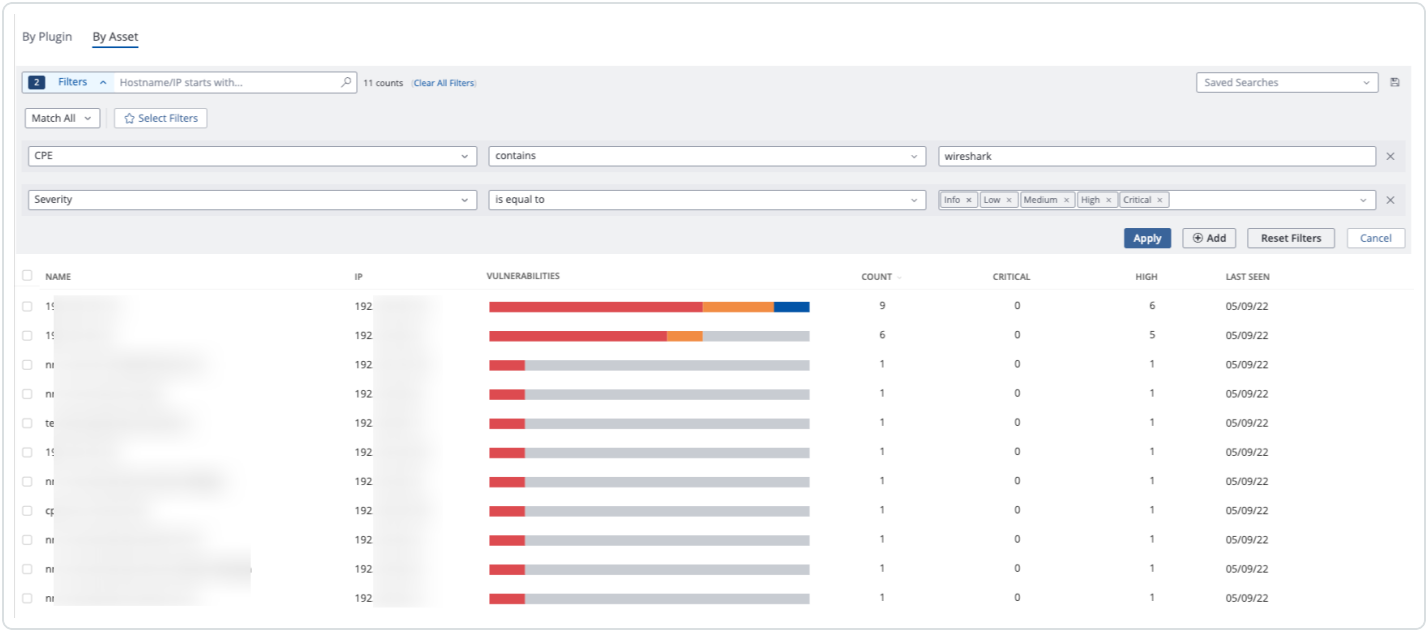
Packet capture software such as Wireshark and tcpdump tend to be authorized for a small group of users within the organization. Tenable's software enumeration plugins can assist in discovering the use of this type of software and reducing the number of authorized installations.

The following images display results matching the filter: *CPE* **contains** wireshark. The Wireshark CPE is */a:wireshark:wireshark*, so the full CPE can be searched as well. When using only the *CPE* **contains** filter, the results include Wireshark vulnerabilities as well as an informational plugin for the detection of the Wireshark software. Typically, detection-only plugins are *Info* severity, so the *Severity* filter for *Info* can also be applied to display a list of assets with Wireshark installed.

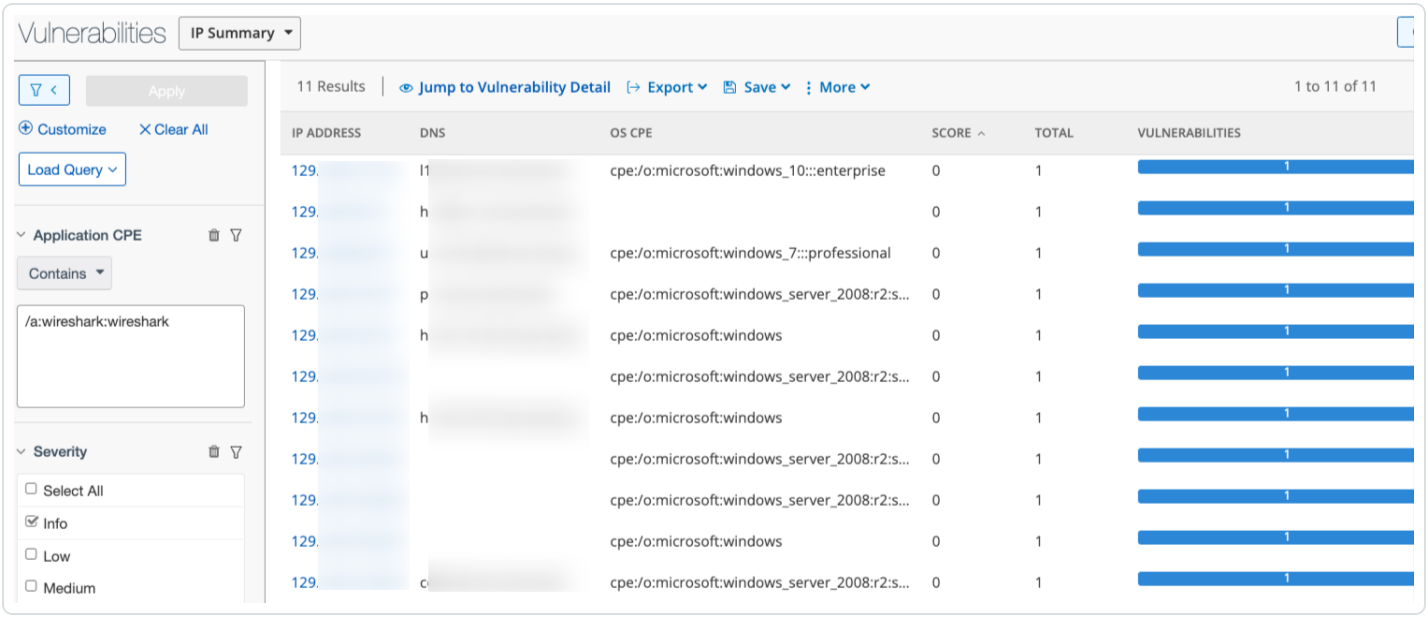
Wireshark Software & Vulnerability Detection in Tenable Security Center



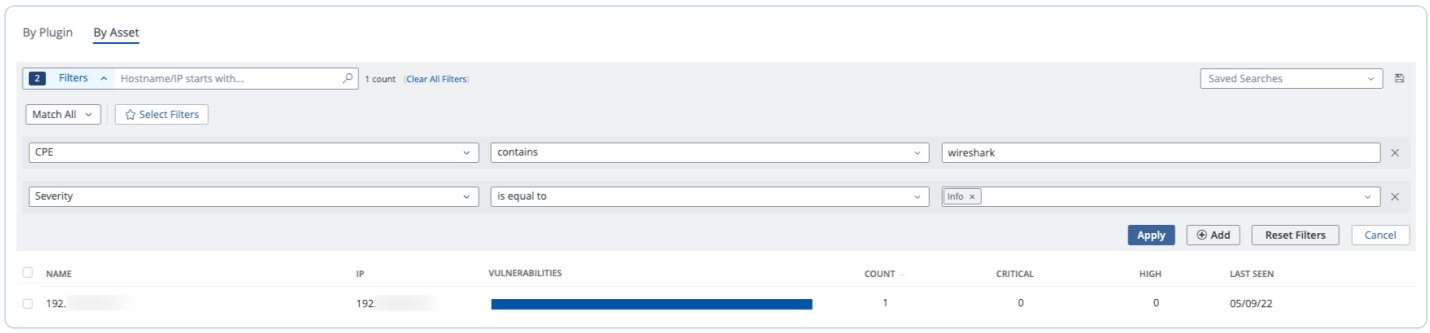
Wireshark Software & Vulnerability Detection in Tenable Vulnerability Management



Wireshark Software Detection in Tenable Security Center



Wireshark Software Detection in Tenable Vulnerability Management



The output of the Common Platform Enumeration (CPE) (45590) plugin provides CPE syntax for operating system and application names that can be used in searches using the *CPE* filter in Tenable Vulnerability Management and the *Application CPE* filter in Tenable Security Center. The **cpe:/a:** syntax represents an application CPE, the **cpe:/o:** syntax represents an operating system CPE, **p-cpe:/** is used for Linux package checks, **cpe:/h:** represents a type of hardware, and **x-cpe:/** is used when NIST does not have a defined CPE. The following is a sample of some of the CPEs from plugin 45590:

- cpe:/a:microsoft:.net_framework:3.0 -> Microsoft .NET Framework 3.0
- cpe:/a:microsoft:.net_framework:4.8
- cpe:/a:microsoft:ie:11.0.9600.19596
- cpe:/a:microsoft:internet_information_services:7.5.7600.16385
- cpe:/a:microsoft:remote_desktop_connection:6.1.7601.24543
- cpe:/a:microsoft:system_center_endpoint_protection:4.10.0209.0
- cpe:/a:mozilla:firefox:79.0.0
- cpe:/a:oracle:jre:1.8.0_171
- cpe:/a:tenable:nnm:5.6.0
- cpe:/a:vmware:vcenter_converter:6.2.0
- cpe:/a:vmware:vmware_tools:10.2.0.1608
- cpe:/a:vmware:vsphere_client:
- cpe:/a:apache:http_server:2.4.48 -> Apache Software Foundation Apache HTTP Server
- cpe:/a:apple:safari:15.1 -> Apple Safari

- cpe:/a:openbsd:openssh:8.6 -> OpenBSD OpenSSH
- cpe:/a:redhat:ansible -> Red Hat Ansible
- cpe:/a:vmware:tools:11.2.6.28747 -> VMWare Tools
- cpe:/a:::6.2.3.15-39
- cpe:/a:apache:http_server -> Apache Software Foundation Apache HTTP Server
- cpe:/a:cisco:firepower_threat_defense:6.2.3.15.39 -> Cisco Firepower Threat Defense (FTD)
- cpe:/a:cisco:firepower_threat_defense:6.2.3.15_(build_39) -> Cisco Firepower Threat Defense (FTD)
- cpe:/a:openbsd:openssh:7.4 -> OpenBSD OpenSSH 7.4
- x-cpe:/a:microsoft:dhcp_server:6.1.7601.24498
- x-cpe:/a:tenable:log_correlation_engine_client:windows:5.0.1.0
- x-cpe:/a:slack:slack
- cpe:/o:apple:mac_os_x:12.0.1 -> Apple Mac OS X
- cpe:/o:cisco:ios_xe
- cpe:/o:linux:linux_kernel:4.4
- cpe:/o:cisco:ios:15.5 -> Cisco IOS
- cpe:/o:cisco:ios_xe:16.6.3 -> Cisco IOS XE
- cpe:/h:dell:remote_access_card:8 -> Dell Remote Access Card

Plugin Output for Plugin ID 45590 in Tenable Security Center

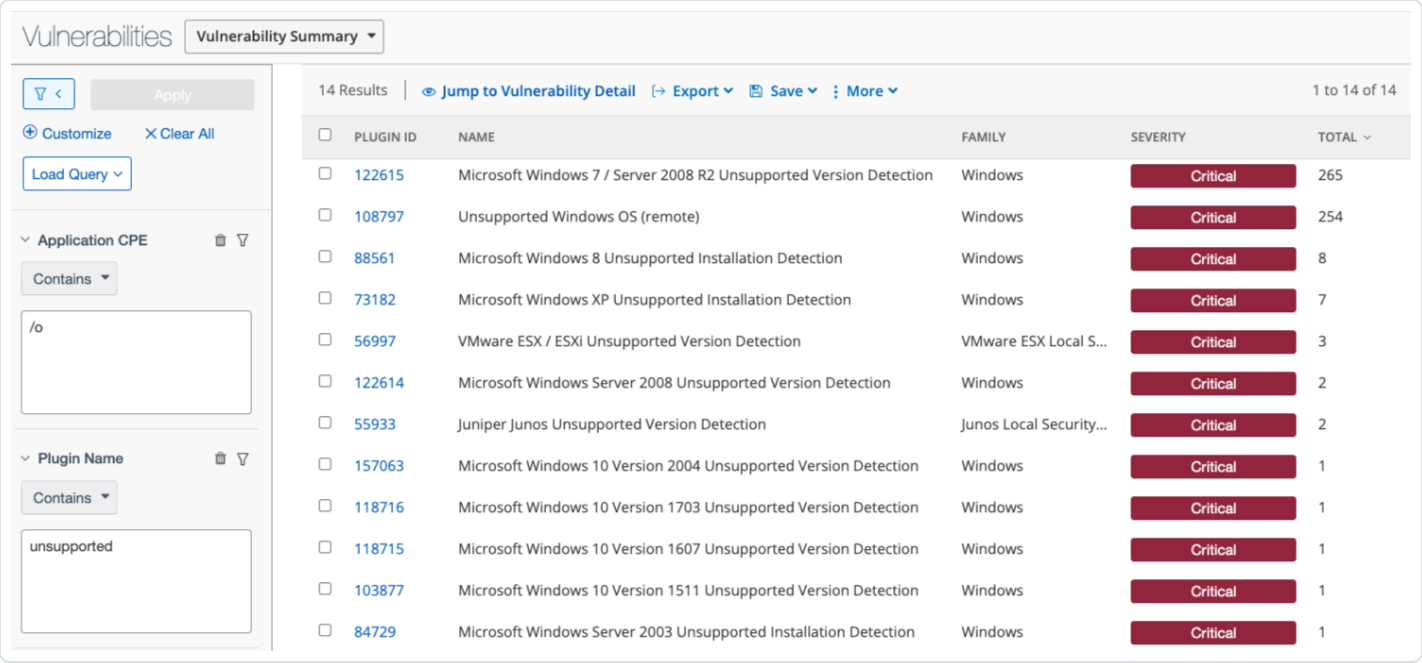
```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE matched on the remote system :

  cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH

Following hardware CPE matched on the remote system :

  cpe:/h:dell:remote_access_card:8 -> Dell Remote Access Card
```

```
The remote operating system matched the following CPE :

  cpe:/o:linux:linux_kernel -> Linux Kernel

Following application CPE's matched on the remote system :

  cpe:/a:apache:http_server:2.4.27 -> Apache Software Foundation Apache HTTP
Server
  cpe:/a:openssl:openssl:1.0.2k -> OpenSSL Project OpenSSL

Following hardware CPE matched on the remote system :

  cpe:/x-cpe:/h:axis:network_camera
```

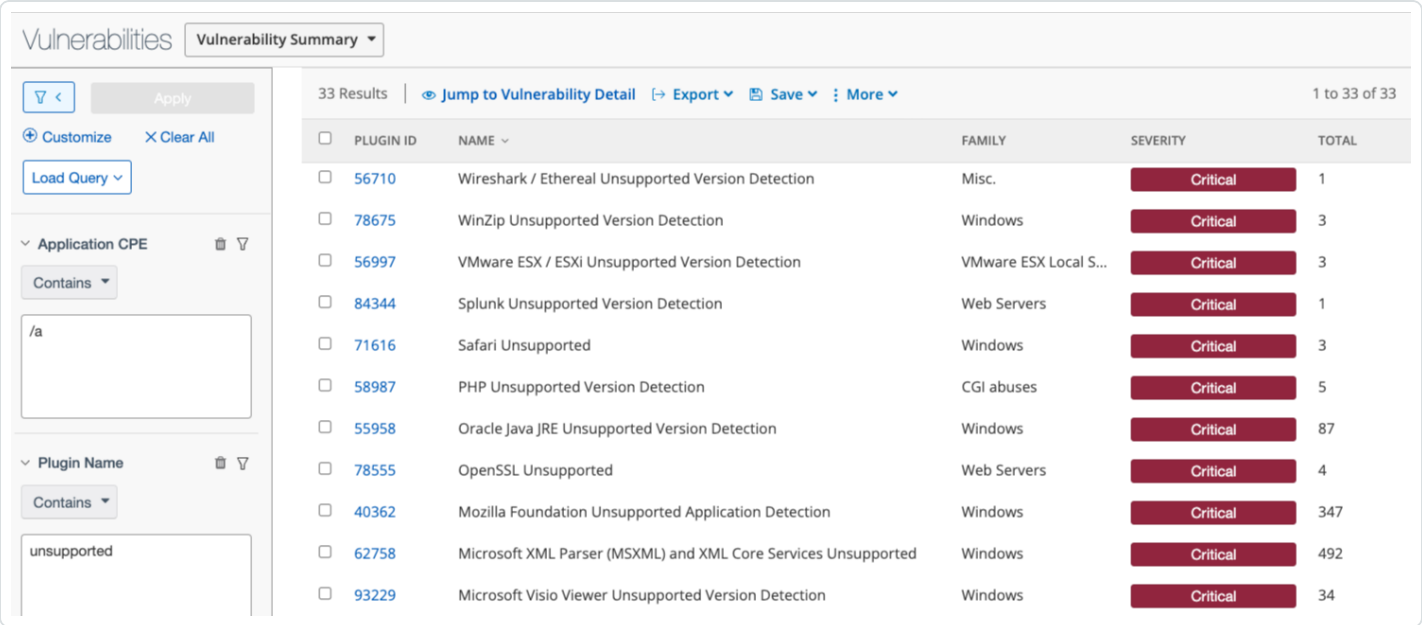
```
Following application CPE's matched on the remote system :

  cpe:/a:lighttpd:lighttpd:1.4.33 -> lighttpd
  cpe:/a:openbsd:openssh:6.6 -> OpenBSD OpenSSH
  cpe:/a:samba:samba:4.3.11 -> Samba Samba

Following hardware CPE matched on the remote system :

  cpe:/x-cpe:/h:buffalotech:terastation
```

The *Unsupported Product Summary - Applications* and *Unsupported Product Summary - All OSes* Tenable Security Center Dashboard Components use the following filters to report unsupported operating systems and applications:

- *Application CPE* **contains** /o
- *Plugin Name* **contains** unsupported



- *Application CPE* **contains** /a
- *Plugin Name* **contains** unsupported

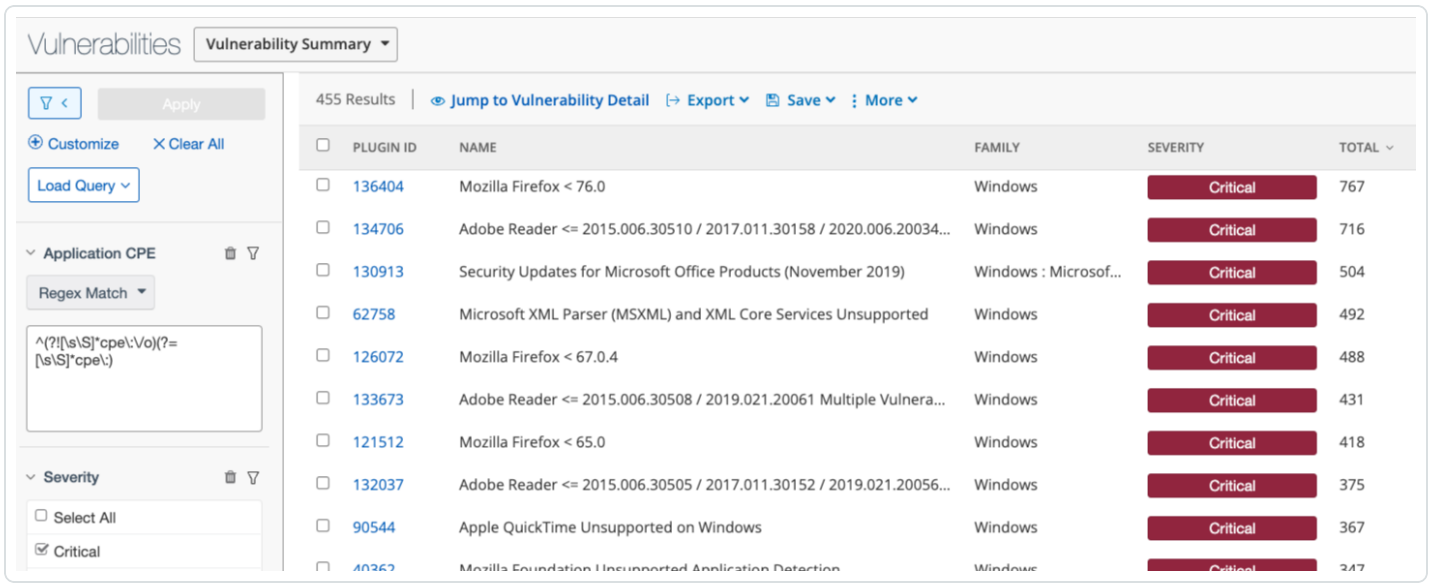


Filter Spotlight: The **Regex Match** operator can be used to perform more complex searches with the Application CPE filter, as shown below. The *ASD Top 4 Mitigation Strategies - Active OS* and *Application Vulnerability Counts* Tenable Security Center Dashboard Component uses the *Application CPE* regex matches described below.

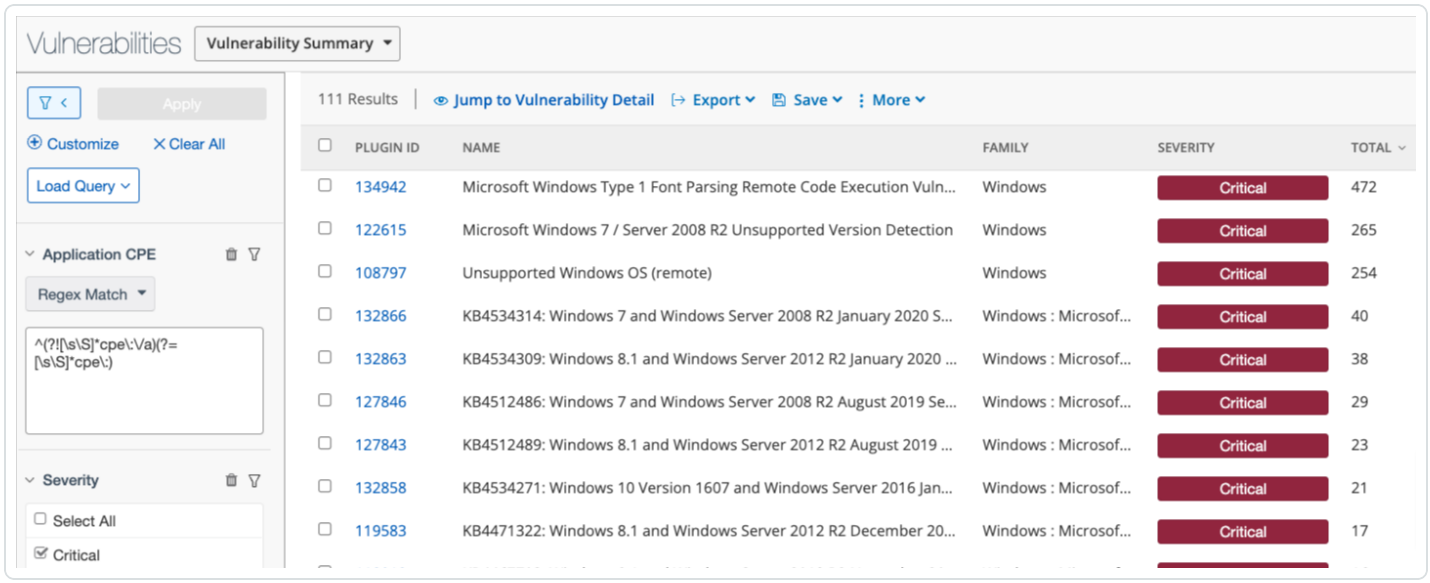
ASD Top 4 Mitigation Strategies - Active OS and Application Vulnerability Counts

	Medium	High	Critical	Exploitable
Apps Only	33384	34368	15239	29160
OS Only	3460	7067	1475	7475
OS & Apps	7472	3320	441	4894
No CPE	14856	1031	26	566
Total	59155	45777	17173	42095

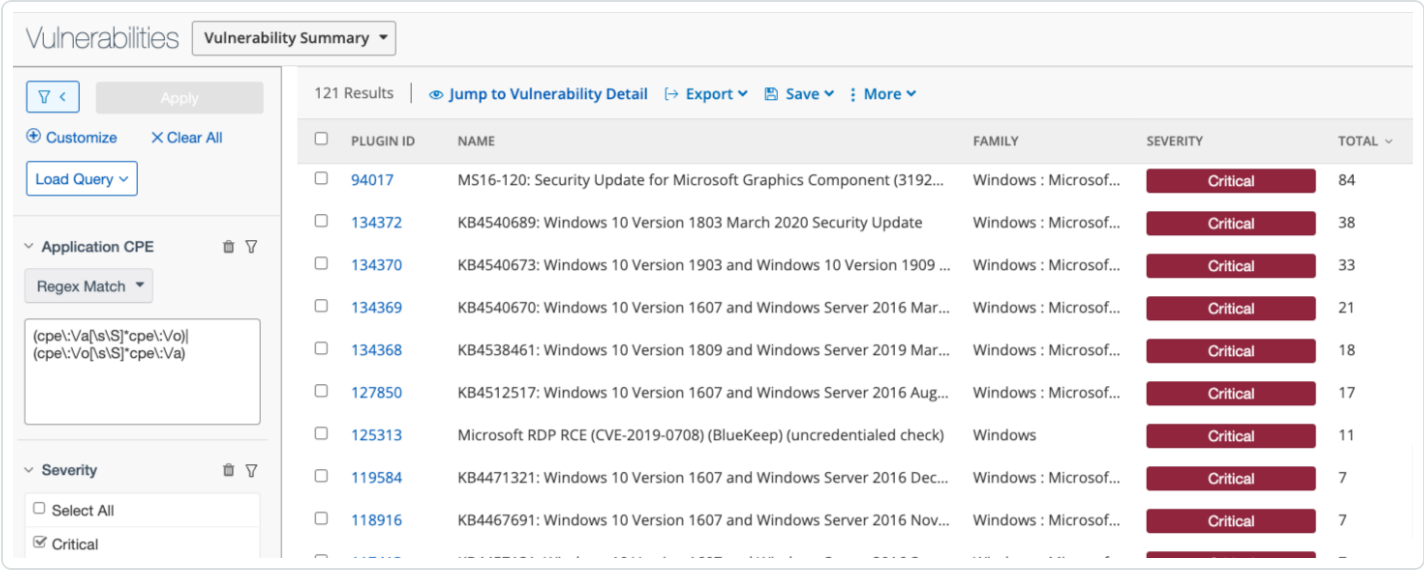
Apps Only: *Application CPE* **Regex Match** ^(?![\s\S]*cpe\:\/o)(?=[\s\S]*cpe\:)



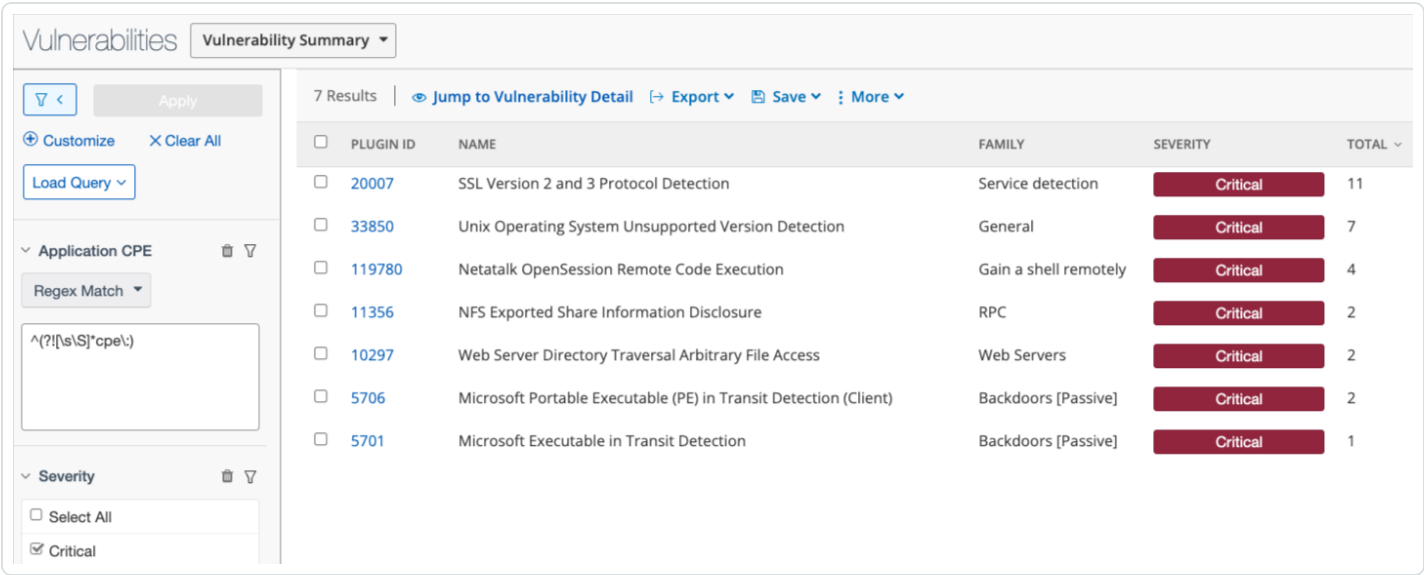
OS Only: *Application CPE* **Regex Match** ^(?![\s\S]*cpe\:\/a)(?=[\s\S]*cpe\:)



OS & Apps: *Application CPE* **Regex Match** (cpe\:\/a[\s\S]*cpe\:\/o)(cpe\:\/o[\s\S]*cpe\:\/a)



No CPE: *Application CPE* **Regex Match** ^(?![\s\S]*cpe\:)



Grouping Assets

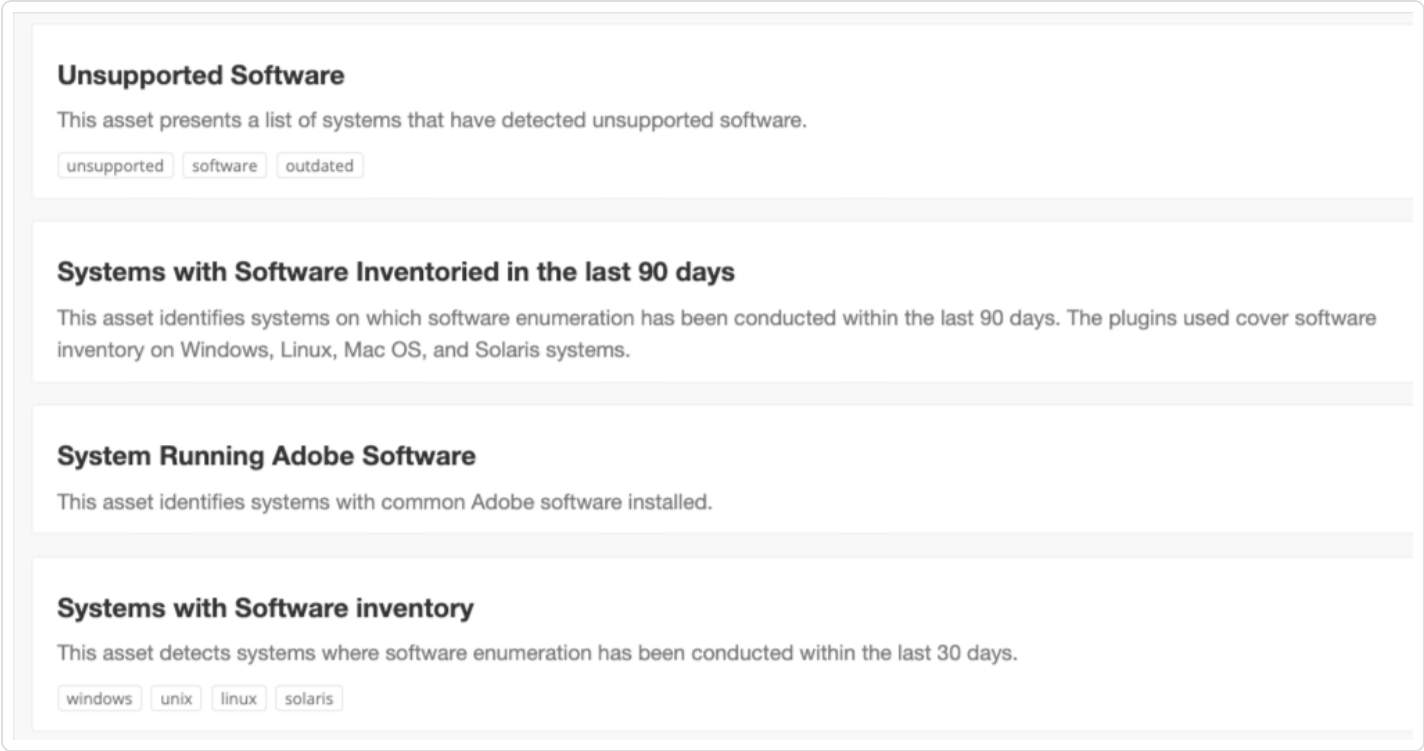
Grouping assets by common functions and features, such as Operating System, platform, or business function facilitates vulnerability scanning and remediation by ensuring that scans are configured to probe for common weaknesses in the platform or application. Systems may be classified in multiple asset lists. For example, a Linux web server on the DMZ may be listed under “Linux Systems,” “Web Servers,” and “DMZ Systems.” This classification ensures that scans are targeted appropriately. Create asset lists that logically group assets, such as:

- Critical business servers
- Critical infrastructure devices
- Managed servers
- User / Desktop
- Off-site (VPN, Managed)
- Production servers
- Development servers
- Test systems

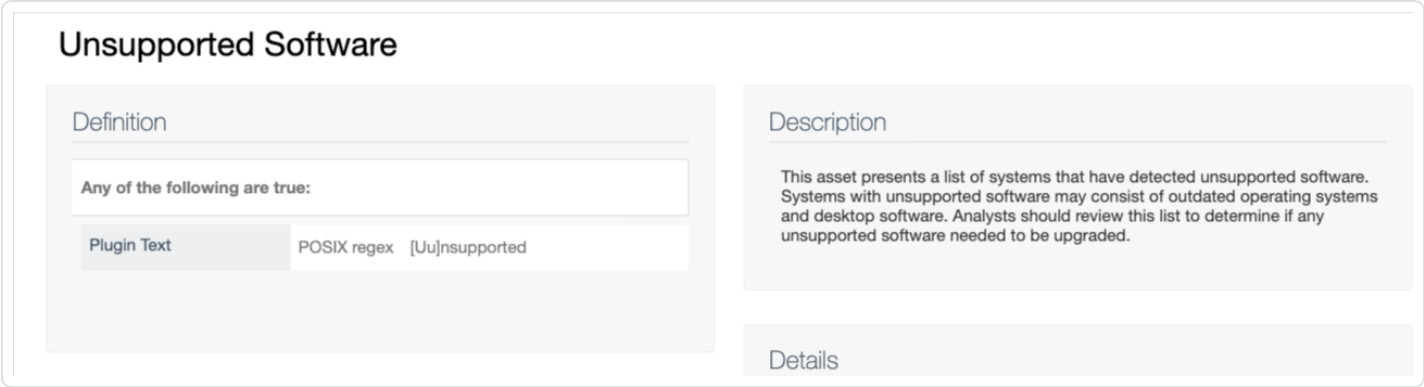
Maintaining a software inventory provides visibility into assets that align with specific software categories. This enables tracking assets with authorized, unauthorized, or unsupported software. Assets can be grouped in Tenable Vulnerability Management using Tags and in Tenable Security Center using Dynamic Assets.

Grouping Assets in Tenable Security Center

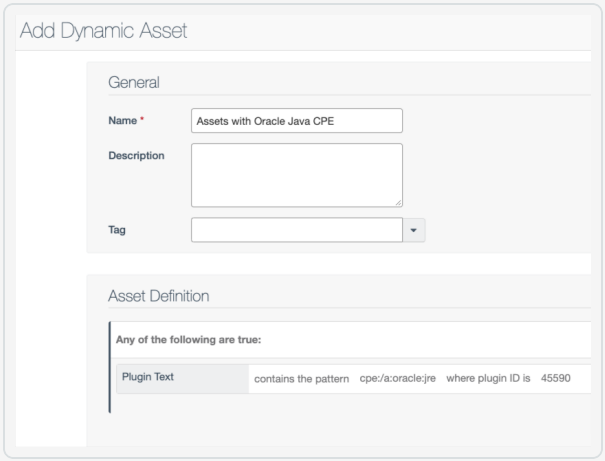
There are hundreds of built-in Asset templates in Tenable Security Center. A search for the word "software" displays a few of the asset templates, as shown below:



The *Unsupported Software* Asset template in Tenable Security Center uses a POSIX regex filter for Plugin Text (also known as vulnerability text or plugin output).



Custom Dynamic Assets can be created in Tenable Security Center using the filters in the list below. A good example is to use *Plugin Text* **contains** *cpe:/a:oracle:jre* where *plugin ID* **is** *45590*.

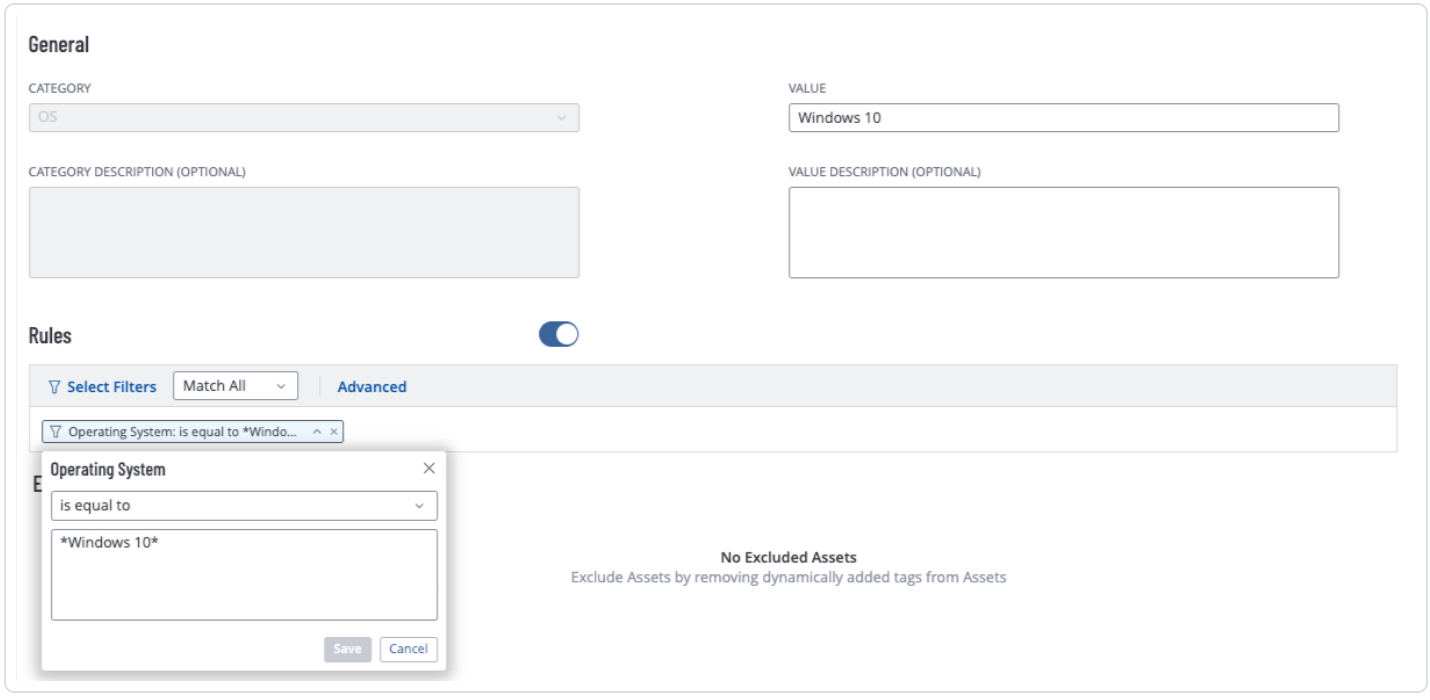


- Agent ID
- Plugin ID
- Plugin Text (Vulnerability Text or Plugin Output)
- Operating System
- IP Address
- DNS
- NetBIOS Host
- NetBIOS Workgroup
- MAC
- SSH v1 Fingerprint
- SSH v2 Fingerprint
- Port
- TCP Port

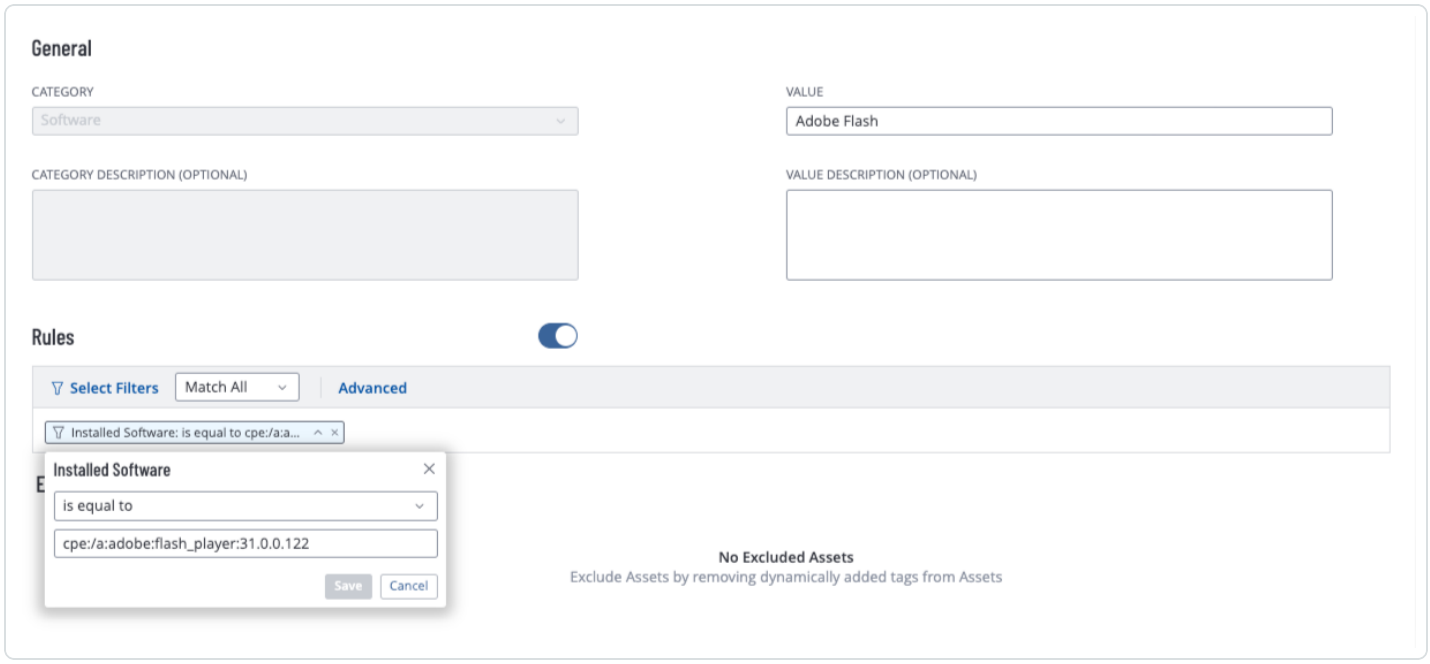
	• UDP Port • Days Since Discovery • Days Since Observation • Severity • Exploit Available • Exploit Frameworks • XRef

Grouping Assets in Tenable Vulnerability Management

Assets can be grouped using Tags in Tenable Vulnerability Management. Dynamic tags are created using many of the filters that are available in Tenable Vulnerability Management. The following example displays the configuration for a tag that groups assets with a Windows 10 Operating System.



The CPE value can also be used to group assets by software installed, as shown in the following image for Adobe Flash.



Verifying Patches

The information that Tenable plugins provide to enumerate software versions can be used to verify that authorized software is updated with the latest patches. The Patch Report (66334) Plugin summarizes a list of patches that need to be installed and enabled on an asset. Use this plugin to track how often a patch assessment is made over time or to extract the data to perform analysis.

The following image is the plugin output from plugin 66334 for a Windows asset:

Plugin Output

```
. You need to take the following 4 actions :
+ Install the following Microsoft patch :
- KB5011495 (56 vulnerabilities)
[ Docker for Windows stable < 18.06.0-ce-win70 / edge < 18.06.0-ce-rc3-win68 Remote Privilege Escalation Vulnerability (117358) ]
+ Action to take : Upgrade to Docker for Windows stable 18.06.0-ce-win70 or edge 18.06.0-ce-rc3-win68 or later.

[ PuTTY < 0.71 Multiple Vulnerabilities (123418) ]
+ Action to take : Upgrade to PuTTY version 0.71 or later.
+Impact : Taking this action will resolve 5 different vulnerabilities (CVEs).


[ VMware Tools 10.2.x / 10.3.x < 10.3.10 Information Disclosure / Denial of Service Vulnerability (VMSA-2019-0009) (125884) ]
+ Action to take : Upgrade to VMware Tools version 10.3.10 or later.
```

The following image is the plugin output from plugin 66334 for a Mac OS Asset:

Plugin Output

```
. You need to take the following 3 actions :

[ Apache 2.4.x < 2.4.53 Multiple Vulnerabilities (158900) ]
+ Action to take : Upgrade to Apache version 2.4.53 or later.
+Impact : Taking this action will resolve 39 different vulnerabilities (CVEs).


[ Tenable Nessus 10.x < 10.1.2 / 8.x < 8.15.4 Third-Party Vulnerability (TNS-2022-06) (159376) ]
+ Action to take : Upgrade to Tenable Nessus version 10.1.2 or 8.15.4 or later.
+Impact : Taking this action will resolve 24 different vulnerabilities (CVEs).


[ VMware Tools < 11.1.1 Denial-of-Service Vulnerability (VMSA-2020-0014) (macOS) (137839) ]
+ Action to take : Upgrade to VMwware Tools version 11.1.1 or later.
```

The following image is the plugin output from plugin 66334 for Linux Asset:

Plugin Output

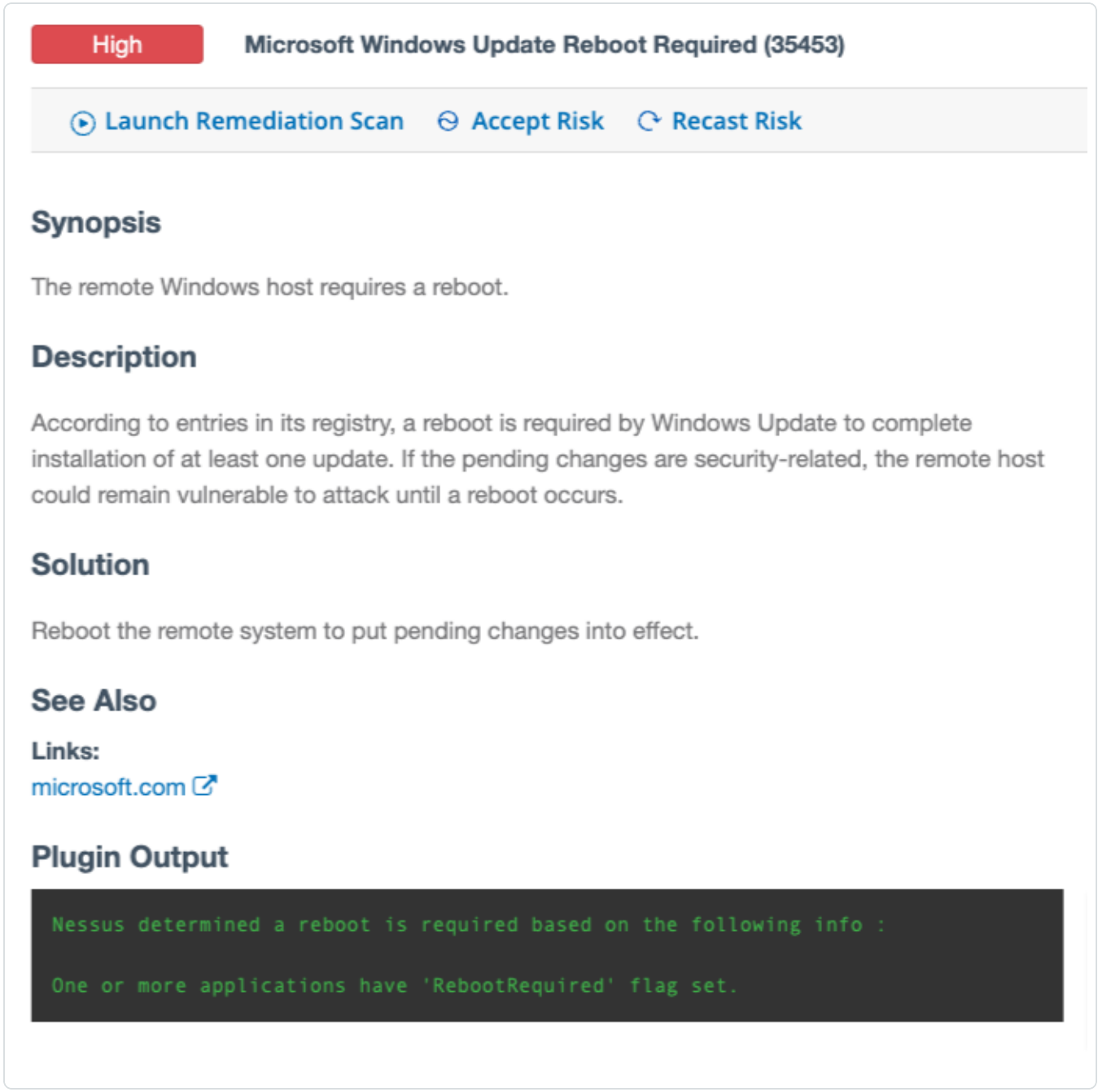
```
. You need to take the following 38 actions :

[ CentOS 5 / 6 / 7 : openldap (CESA-2015:1840) (86515) ]

+ Action to take : Update the affected openldap packages.

[ CentOS 5 / 6 : rpm (CESA-2014:1974) (79843) ]

+ Action to take : Update the affected rpm packages.

[ CentOS 5 / 6 : rsyslog / rsyslog5 (CESA-2014:1671) (78607) ]

+ Action to take : Update the affected rsyslog and / or rsyslog5 packages.

[ CentOS 6 / 7 : expat (CESA-2016:2824) (95373) ]

+ Action to take : Update the affected expat packages.

[ CentOS 6 / 7 : libgcrypt (CESA-2016:2674) (94741) ]

+ Action to take : Update the affected libgcrypt packages.

[ CentOS 6 / 7 : net-snmp (CESA-2015:1636) (85464) ]

+ Action to take : Update the affected net-snmp packages.

+Impact : Taking this action will resolve 3 different vulnerabilities (CVEs).
```

Note: There are often instances where a patch has been applied but is still reported in plugin 66334, or the plugin will fire for the individual patch. The patch is still being reported as a vulnerability because although the patch has been applied, another step is required to fully enable the patch. The additional step could require a reboot, a registry key, or a GPO change. Patch management solutions such as SCCM or WSUS may also report the patch as applied and the asset not vulnerable, but Tenable reports the patch as missing because the patch is not fully enabled.

Following are some suggested filters to find these instances of patches that are not fully enabled. Note that Plugin Output in Tenable Vulnerability Management is Vulnerability Text in Tenable Security Center.

- SCCM or WSUS report that patch has been applied
    - *Plugin Output* **contains** SCCM: NOT Vulnerable
    - *Plugin Output* **contains** SCCM: NOT Vulnerable

- Reboot required
    - *Plugin ID* **equals** 35453
    - *Severity* **equals** High



- Registry change required (Tenable Vulnerability Management)
    - *Severity* **equals** Medium, High, Critical
    - *Plugin Output* **contains** HKLM
    - *Plugin Output* **contains** registry

```
The following registry key is required to enable the fix for CVE-2017-8529 and is missing.
  HKLM\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe

The following registry key is required to enable the fix for CVE-2017-8529 and is missing.
  HKLM\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe
```

- Registry change required (Tenable Security Center)
    - *Severity* **equals** Low, Medium, High, Critical
    - Only required in Tenable Security Center: *Plugin Type* **equals** Active
    - *Vulnerability Text* **Regex Match** HKLM|HKU|HKCU|Registry

```
The registry key
"HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\LdapEnforceChannelBindin
g"
  is missing or is not equal to "1" or "2"
```

Detecting Running 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 that may be running on the system that is not shown in the registry. The plugins below provide visibility into services that may appear only in running processes rather than in installed software packages. The plugins below provide this valuable information.

- 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

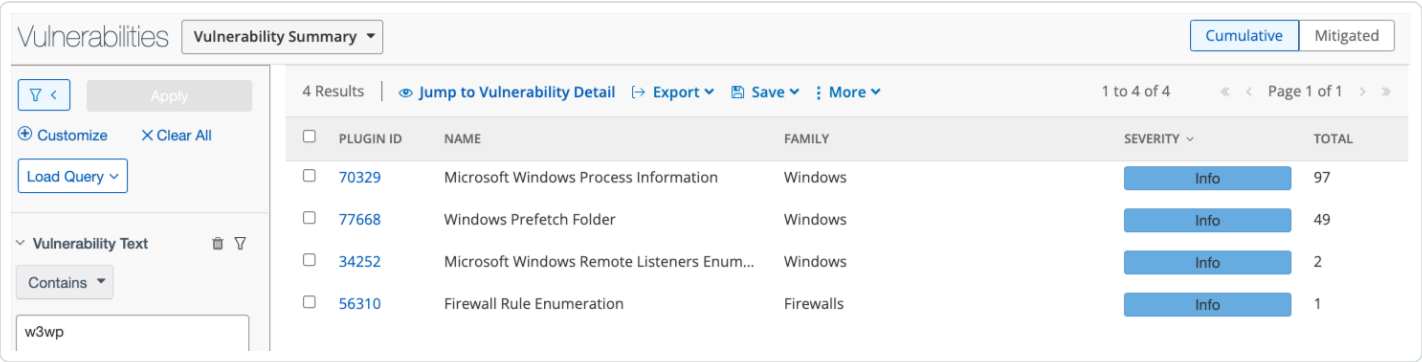
A filter can also be applied using *Plugin Family*: Service Detection.

The following displays sample output for plugin 70329 that 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.

Plugin Output

```
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)
```

The search can be pivoted from *Plugin ID* to *Vulnerability Text*. The following image displays all other scan results that contain *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.



Software Inventory Lifecycle

Software inventory is an ongoing process that needs to be maintained and updated on a regular basis. Maintaining a software inventory aids in cyber hygiene and minimizes unauthorized software installation. Many organizations perform an annual audit by an external third party, where they are required to enumerate authorized software that is running in the environment. Organizations that maintain a current software inventory throughout the year can produce information required by auditors and vendors with minimal effort.

A current software inventory also helps with business roadmap planning. A review of the software running in the environment may reveal that the organization does not have sufficient staffing to support certain services, and outsourcing those services may be more efficient. A review may also reveal that there are services running in the environment that are no longer needed or supported.

Security leaders need to SEE everything, PREDICT what matters most, and ACT to address cyber risk and effectively align cyber security initiatives with business objectives. Tenable Vulnerability Management and Tenable Security Center discover and analyze assets continuously to provide an accurate and unified view of an organization's security posture.

Learn More

Tenable Cyber Exposure

Tenable Blog: Quick Credential Debug Scan

Tenable Blog: The Value of Credentialed Vulnerability Scanning

Tenable Blog: How to Protect Scanning Credentials

Tenable Community Knowledge Base: Nessus Plugin Types and Categories

Tenable Docs: Custom Dynamic Assets

Tenable Docs: Tenable Vulnerability Management Tags

Tenable Plugins Page

Inventory Agent Scanning

FINRA Rules