Tenable Cyber Exposure Study - Malware Defenses

Last Revised: September 26, 2023

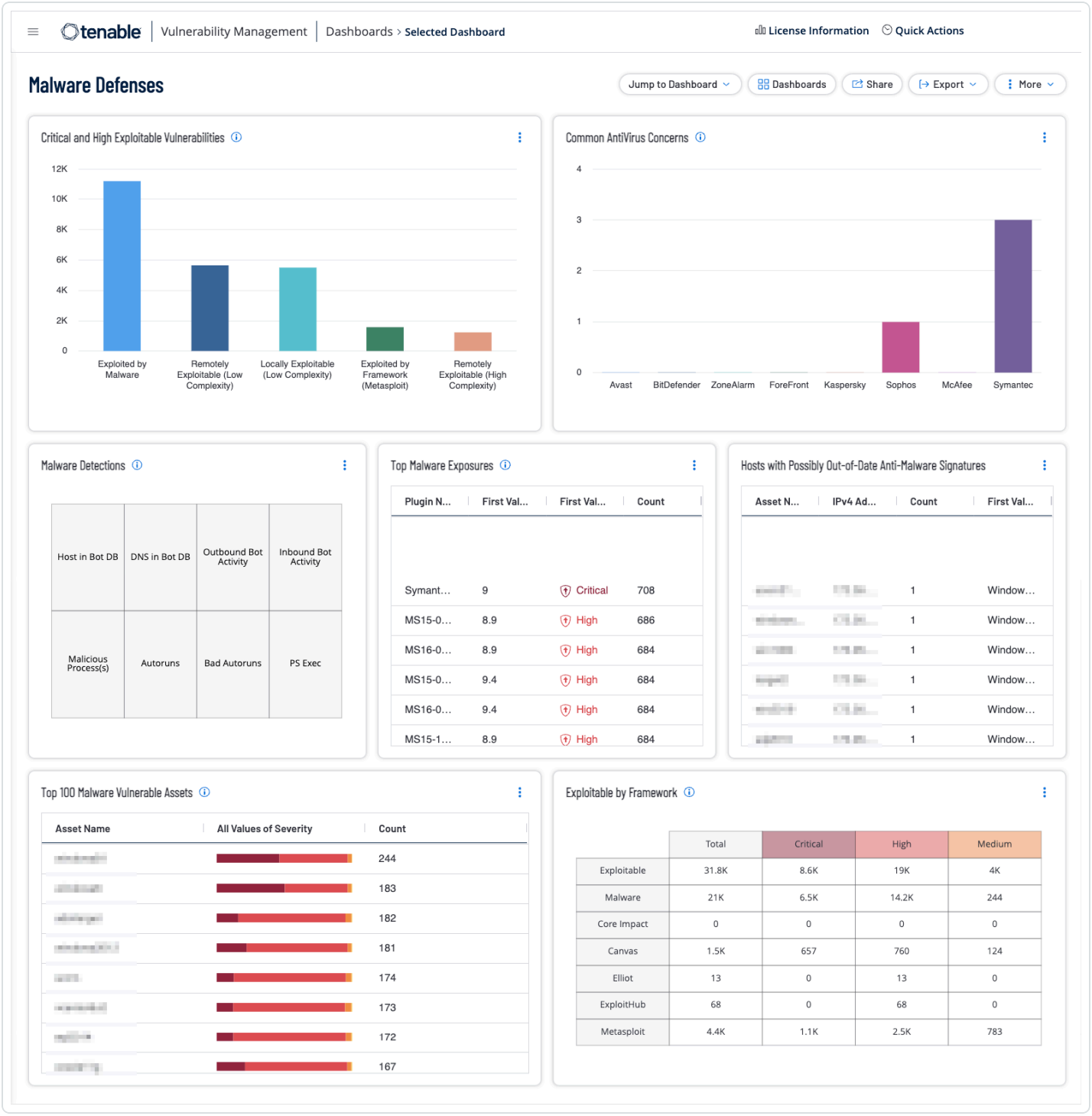
Table of Contents

Overview

Malicious software, or “malware” is software that is designed to cause harm to information systems and is one of the biggest challenges organizations face in maintaining cyber hygiene. Malware exploits weaknesses and vulnerabilities to make software or hardware perform actions not originally intended. Firewalls and other perimeter security devices are designed to protect the organization’s internal network from unauthorized access and malicious attacks. Malware is designed to trick users who have authorized access into running code that provides the attacker access to restricted resources in the internal network. One of the most successful strategies used by malware is to disable host security products, including anti-virus (AV) software. While some anti-virus software has its own control panel for managing host security, reports from the software can be spoofed back to end users and system administrators. In most cases, the report states that the software is installed, but malware has been known to disable AV software while leaving one file or registry entry untouched, so the parent control panel still reports the software as being functional without it actually being operational.

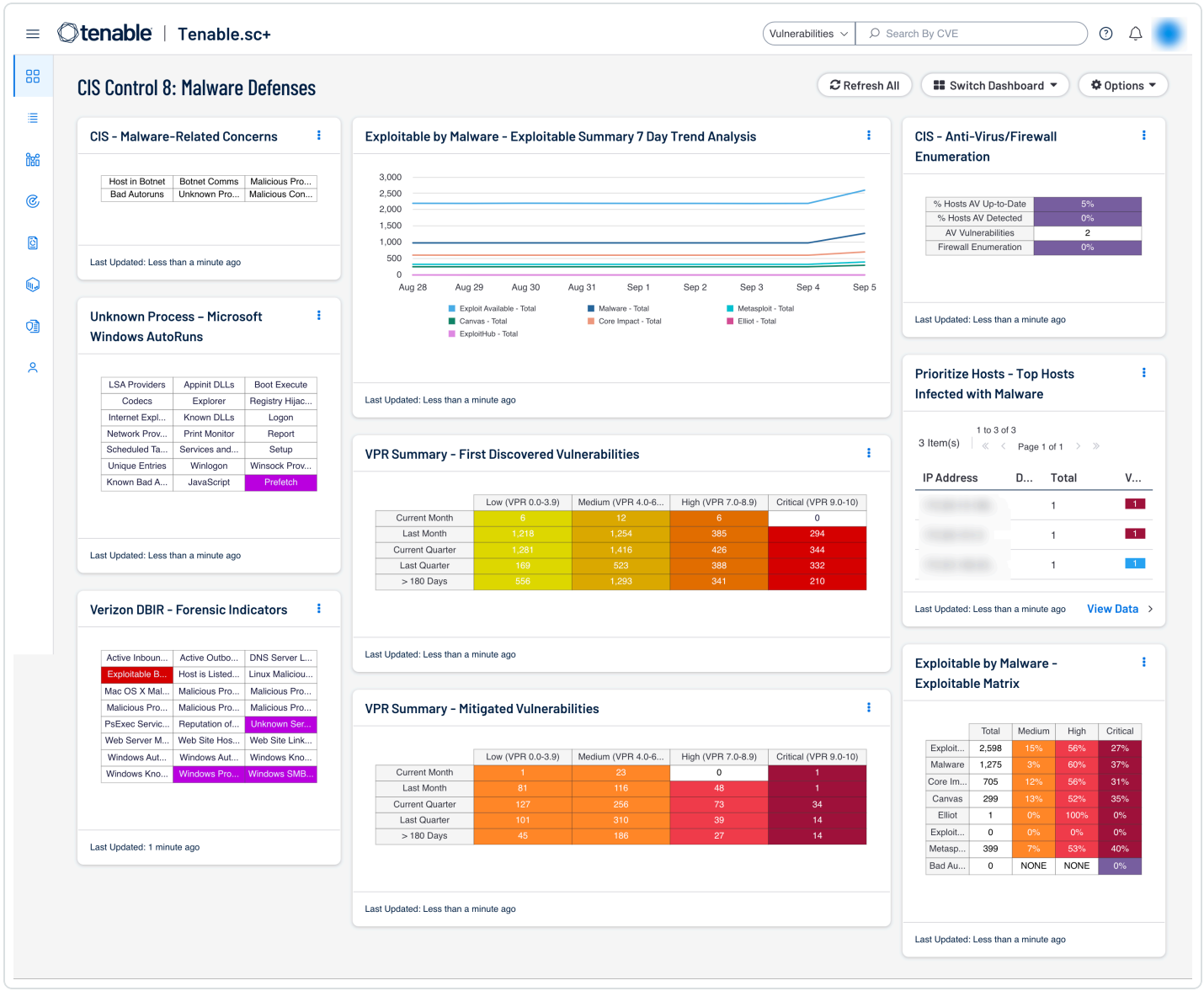
How Tenable Can Help

Tenable Security Center and Tenable Vulnerability Management enables organizations to evaluate vulnerability data gathered from multiple active and passive scanners distributed across the enterprise. The Tenable Vulnerability Management Malware Defenses dashboard provides the necessary context to understand which assets in the organization are vulnerable to malware exploitation.



The Tenable Security Center Malware Defenses dashboard also provides summary status on anti-malware efforts and assets exposed to malware. Organizations need to have controls in place to block malicious application activity. Tenable Security Center has the ability to detect the installation and status of anti-virus programs and to track the vulnerabilities that are exploitable by malware and other exploitation frameworks.

Note: CIS CIS Version 7 listed Anti-Malware as Control 8, which is now mapped to Control 10 in CIS CAS Version 8.



Tenable Security Center and Tenable Vulnerability Management provide organizations a safety net of checks to ensure their antivirus/malware protection is comprehensive and fully functional.

Keeping Anti-Malware Software Up-to-Date

Malware is constantly evolving and the software used to detect the presence of malware must be kept up-to-date to ensure accurate and efficient detection of emerging threats from malicious code. Anti-malware software includes both signature and non-signature methods of detection, and is frequently updated to leverage new advances in technology, such as machine learning and artificial intelligence. New malware is created and released almost daily. Keeping anti-malware software up-to-date involves applying patches when they become available to fix bugs or vulnerabilities and to update to the latest stable version to leverage the latest features. Any signature based anti-malware rules must be updated with the latest signatures from the vendor to ensure the latest known malware is detected.

- Detecting Software Version
- Detecting Out-of-Date Signatures

Detecting Software Version

Plugin 16193 - Antivirus Software Check is the primary plugin that checks to see if antivirus software is installed on the remote host and is up-to-date. Other plugins that check for the presence of anti-malware software include the following:

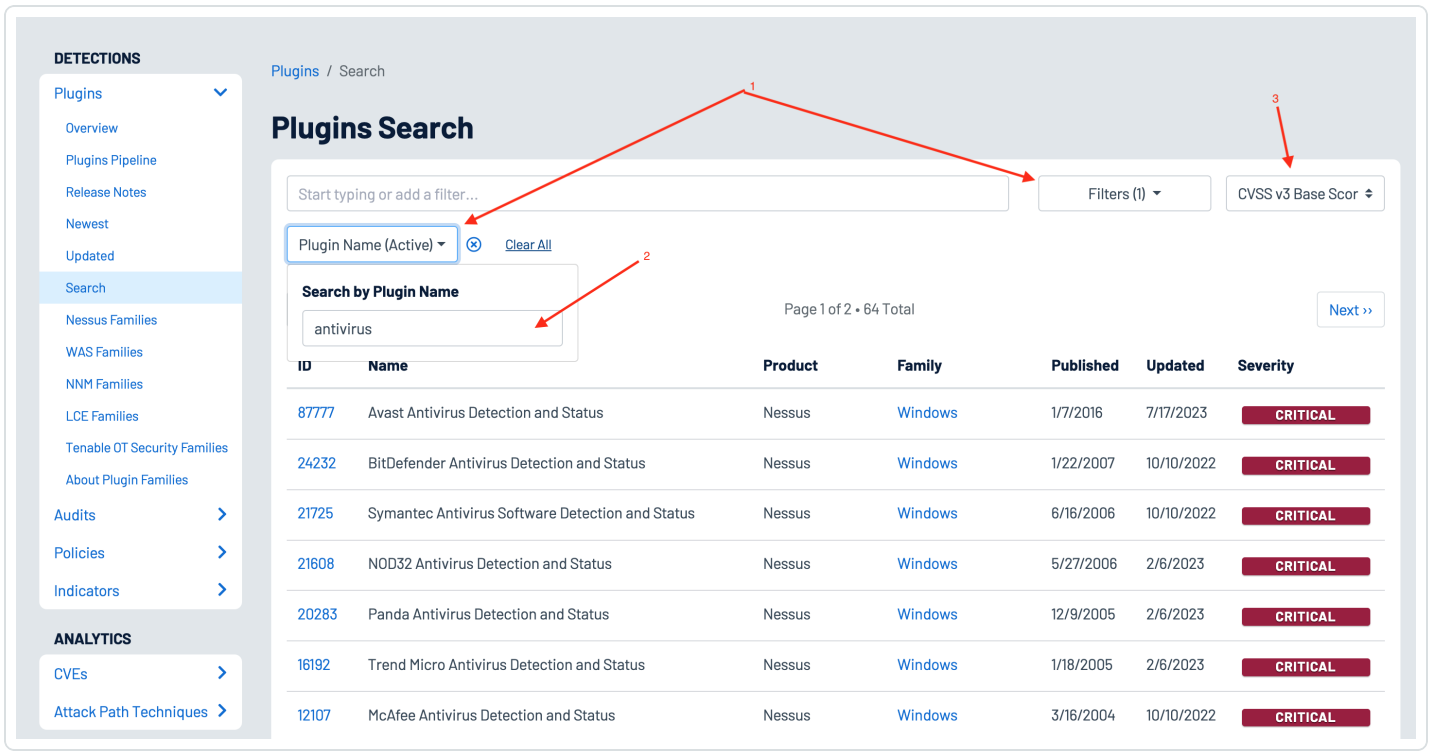
- 84432 AVG Internet Security Detection
- 136761 BitDefender Endpoint Security Tools Detection (Windows)
- 170672 McAfee Total Protection Installed (Windows) windows defender
- 131023 Windows Defender Installed
- 112279 Windows Defender Advanced Threat Protection Installed (Windows)
- 131725 Sophos Anti-Virus Installed (Windows)
- 133962 Sophos Anti-Virus Installed (Linux)
- 54845 Sophos Anti-Virus for Mac OS X Detection
- 58951 Comodo Antivirus / Internet Security Installed
- 22419 Symantec SAVCE/Client Security Service Detection
- 31857 Symantec AntiVirus Scan Engine Detection

Plugin Search Example:

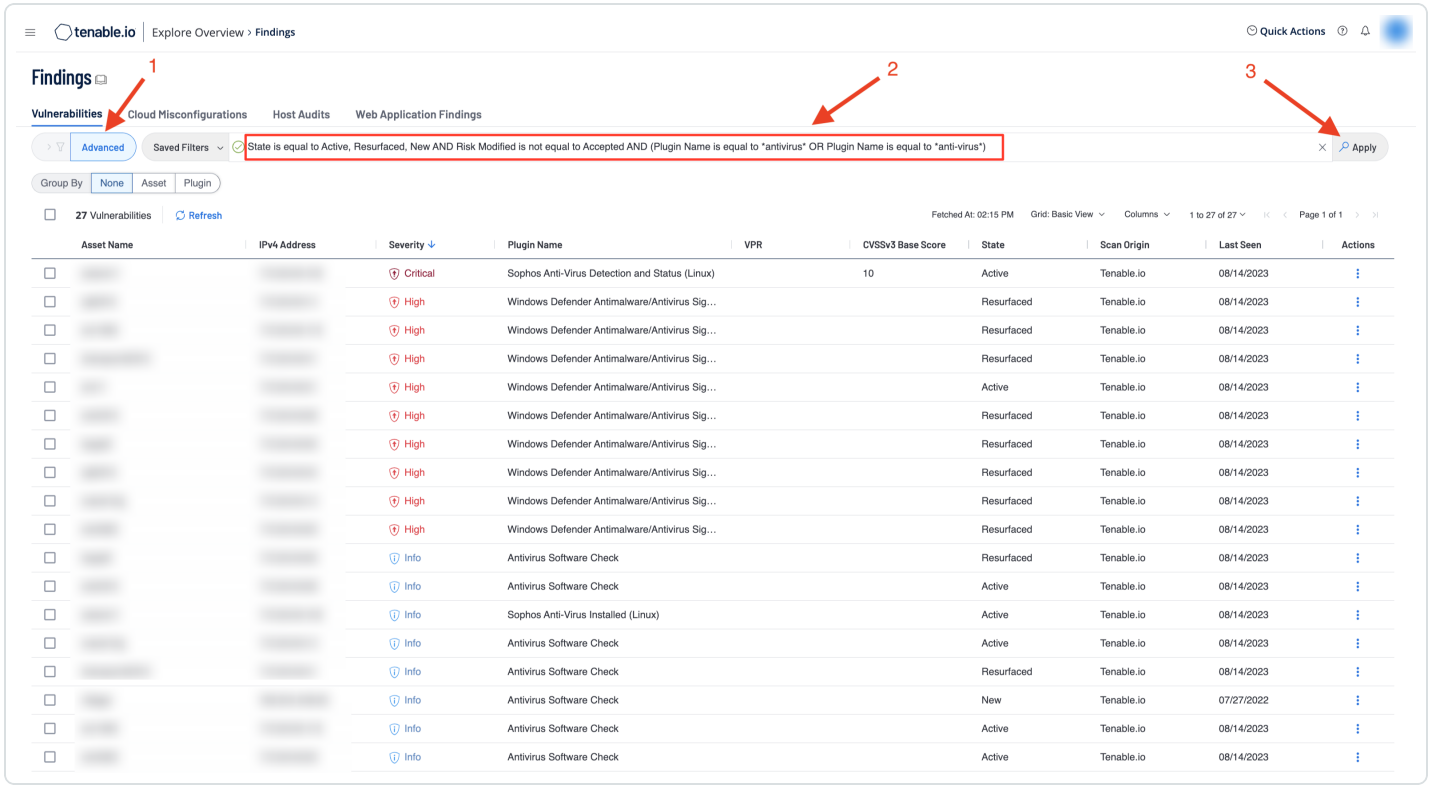
To search for the plugins that detect anti-malware or antivirus software in the environment, navigate to the Tenable Plugin Search page and perform the following steps:

Step 1: Use the Plugin Name filter to identify plugins that contain a specified text

Step 2: Search for plugins that contain the string “anti-malware” or “antivirus” in the plugin Step 3: The Relevance filter (3) can be used to further refine the search for plugins based on the CVSS v3 Base Score



Scan data can be searched on Security Center or Tenable Vulnerability Management to identify antivirus software in the environment. The following image provides an example of performing a filter search from the Findings page in Tenable Vulnerability Management.

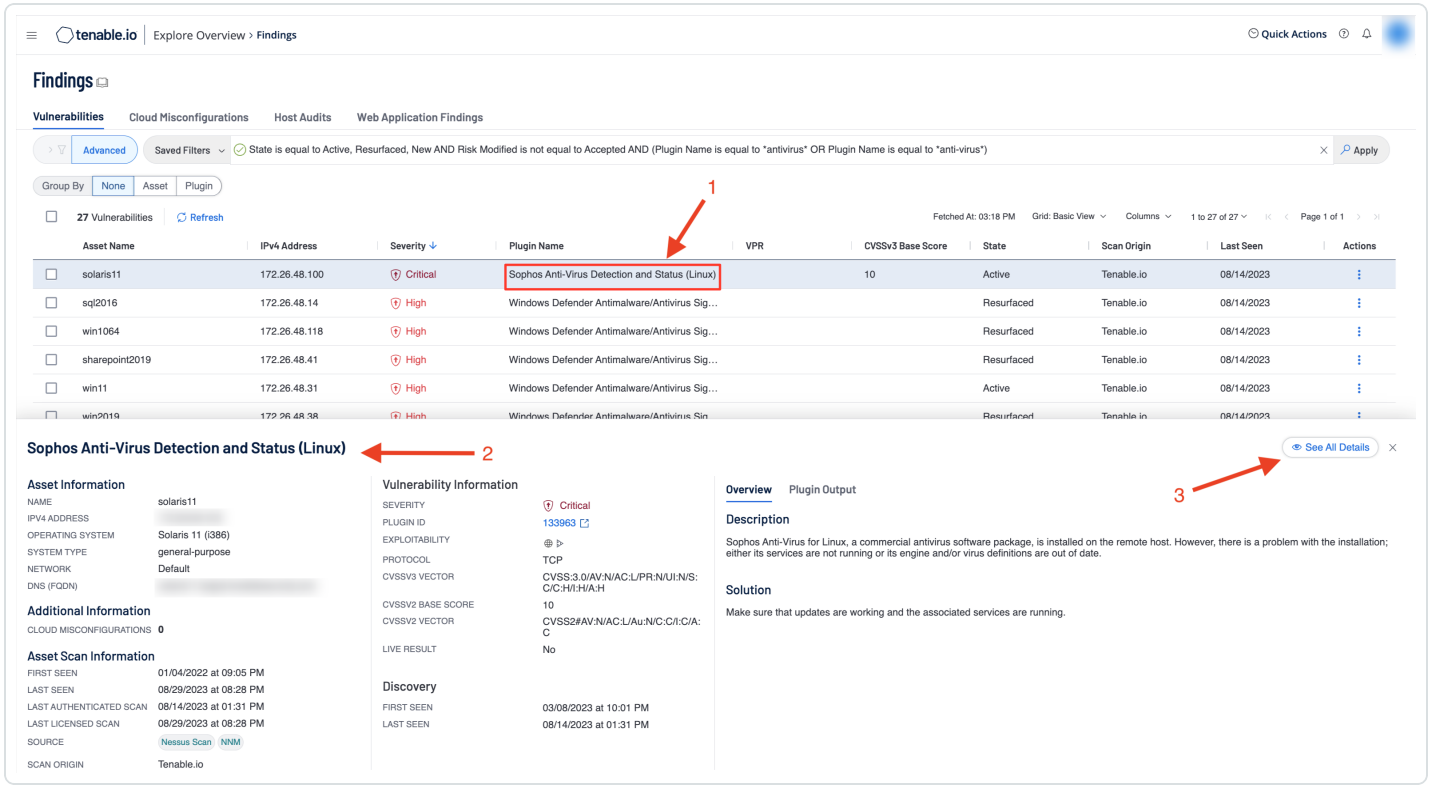


Step 1: Click on the **Advanced** button

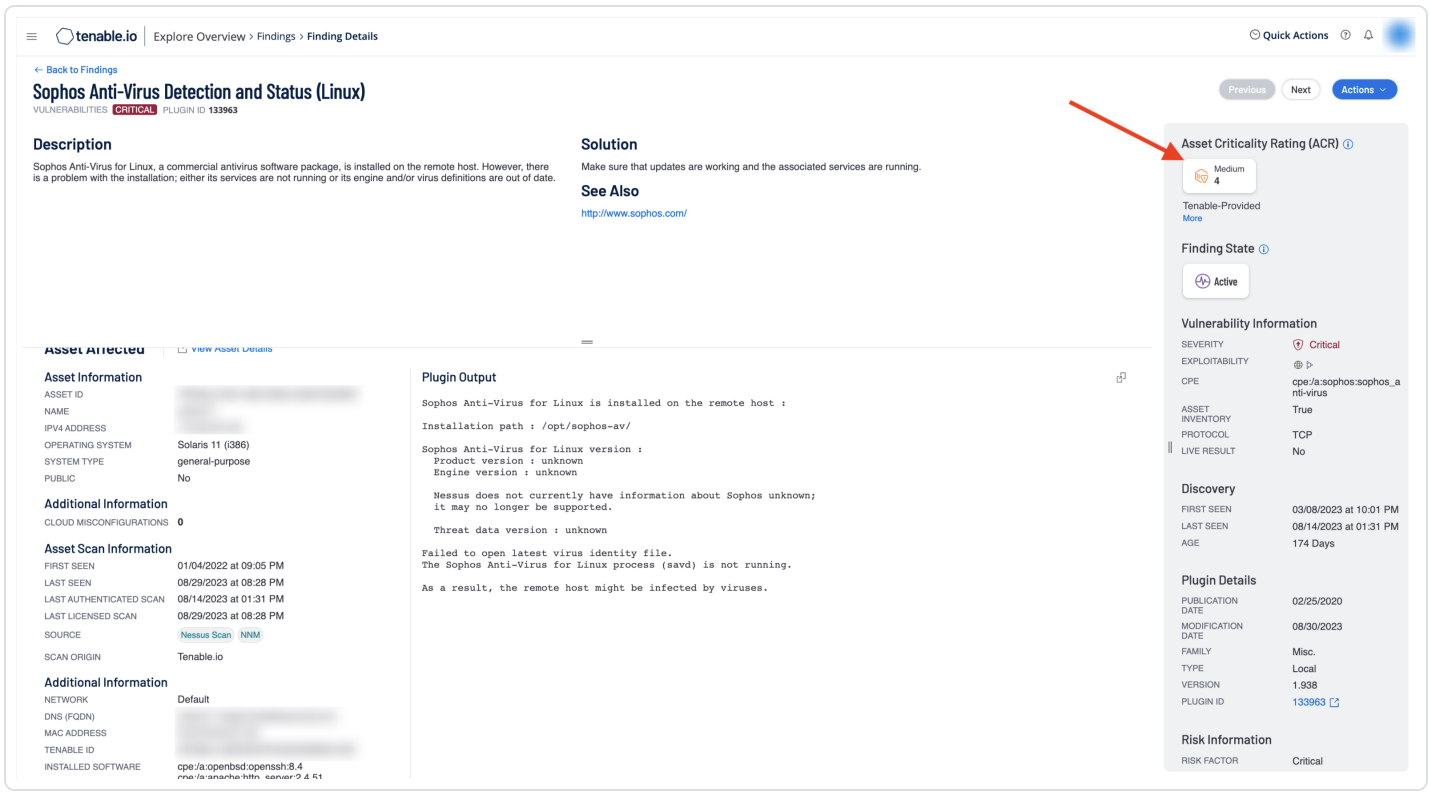
Step 2: Enter the search conditions

Step 3: Click on the Apply button

Click on any of the findings, as shown in **Step 1** in the following image to display more information gathered about the asset for this plugin as shown in **Step 2**.

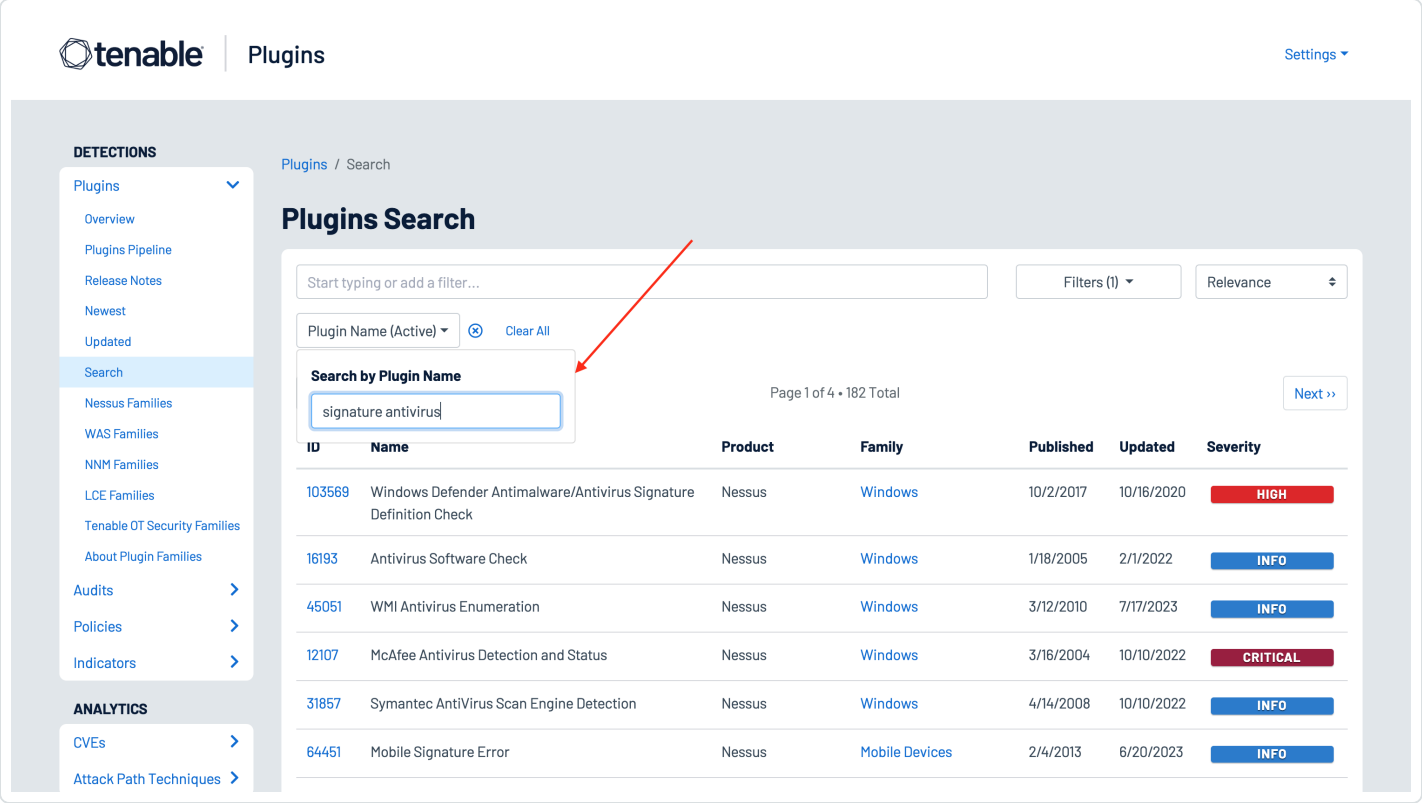


To display further details about the plugin findings, click on the “See All Details” button shown in **Step 3** in the image above, which provides more information about the asset, including the Asset Criticality Rating (ACR). In this example, the ACR is Medium and the Plugin Output indicates that the antivirus solution, while installed, is not running and may no longer be supported.


tenable.io
Explore Overview > Findings > Finding Details
Quick Actions
Back to Findings
Sophos Anti-Virus Detection and Status (Linux)
VULNERABILITIES CRITICAL PLUGIN ID 133963
Previous
Next
Actions
Description
Sophos Anti-Virus for Linux, a commercial antivirus software package, is installed on the remote host. However, there is a problem with the installation; either its services are not running or its engine and/or virus definitions are out of date.
Solution
Make sure that updates are working and the associated services are running.
See Also
http://www.sophos.com/
Asset Criticality Rating (ACR)
Medium 4
Tenable-Provided
More
Finding State
Active
Vulnerability Information
SEVERITY Critical
EXPLOITABILITY
CPE cpe:/a:sophos:sophos_anti-virus
ASSET INVENTORY True
PROTOCOL TCP
LIVE RESULT No
Discovery
FIRST SEEN 03/08/2023 at 10:01 PM
LAST SEEN 08/14/2023 at 01:31 PM
AGE 174 Days
Plugin Details
PUBLICATION DATE 02/25/2020
MODIFICATION DATE 08/30/2023
FAMILY Misc.
TYPE Local
VERSION 1.938
PLUGIN ID 133963
Risk Information
RISK FACTOR Critical
Asset Information
ASSET ID
NAME
IPV4 ADDRESS
OPERATING SYSTEM Solaris 11 (i386)
SYSTEM TYPE general-purpose
PUBLIC No
Additional Information
CLOUD MISCONFIGURATIONS 0
Asset Scan Information
FIRST SEEN 01/04/2022 at 09:05 PM
LAST SEEN 08/29/2023 at 08:28 PM
LAST AUTHENTICATED SCAN 08/14/2023 at 01:31 PM
LAST LICENSED SCAN 08/29/2023 at 08:28 PM
SOURCE Nessus Scan NNM
SCAN ORIGIN Tenable.io
Additional Information
NETWORK Default
DNS (FQDN)
MAC ADDRESS
TENABLE ID
INSTALLED SOFTWARE cpe:/a:openbsd:openssh:8.4
Plugin Output
Sophos Anti-Virus for Linux is installed on the remote host :
Installation path : /opt/sophos-av/
Sophos Anti-Virus for Linux version :
Product version : unknown
Engine version : unknown
Nessus does not currently have information about Sophos unknown;
it may no longer be supported.
Threat data version : unknown
Failed to open latest virus identity file.
The Sophos Anti-Virus for Linux process (savd) is not running.
As a result, the remote host might be infected by viruses.

Detecting Out-of-Date Signatures

To identify plugins that detect outdated signatures, navigate to the Tenable Plugin Search page and use the Plugin Name filter to search for the terms “signature” and “antivirus”, as shown below:

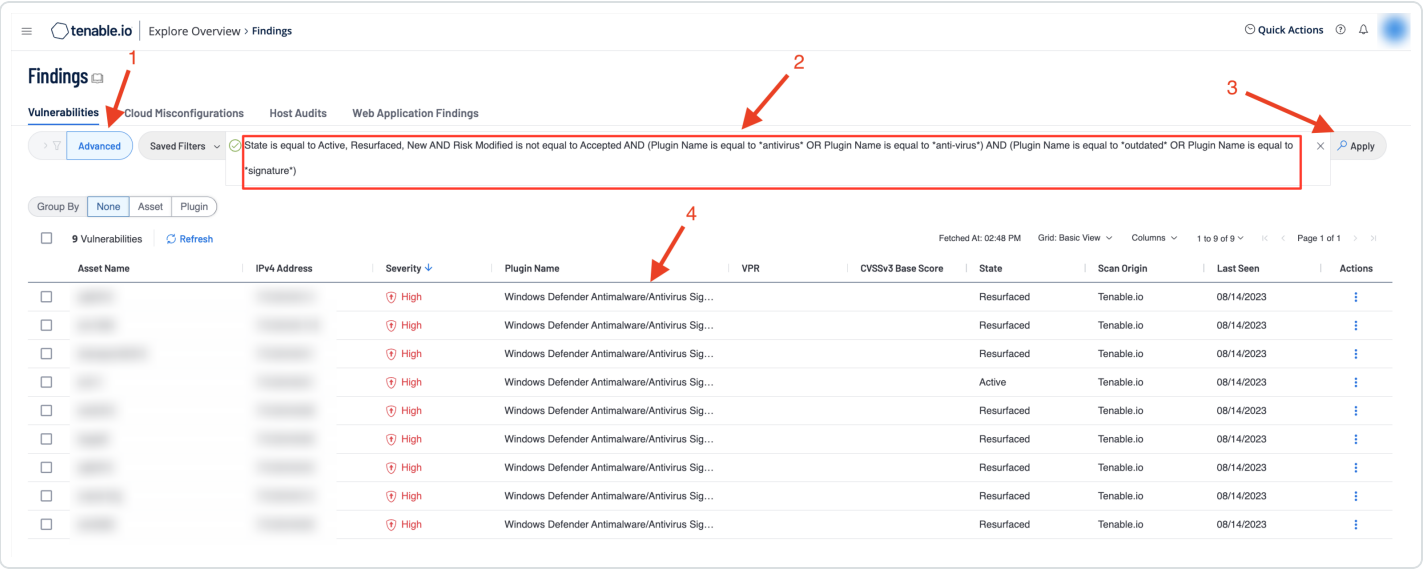


Plugin ID 103569 Windows Defender Antimalware/Antivirus Signature Definition Check is one of the plugins that detect outdated signatures in the environment. Others include the following:

- 88932 AVG Internet Security Out-of-Date
- 24232 BitDefender Antivirus Detection and Status
- 100784 McAfee Antivirus Engine Out of Date
- 24344 Windows Live OneCare Antivirus Detection
- 12215 Sophos Anti-Virus Detection and Status
- 133963 Sophos Anti-Virus Detection and Status (Linux)
- 54846 Sophos Anti-Virus Detection and Status (Mac OS X)

Example Filter Query:

Scan data can be searched on Security Center or Tenable Vulnerability Management to identify outdated virus signatures. The following image provides an example of an Advanced query in from the Findings page in Tenable Vulnerability Management. This example demonstrates how a security analyst can drill into details using advanced filters to customize searches.



Step 1: Click on the Advanced button to enable editing of the conditions filter

Step 2: Modify the displayed search conditions to search for the desired text strings. In this example, the search was performed with the following filter:

```
State is equal to Active, Resurfaced, New AND Risk Modified is not equal to Accepted AND (Plugin Name is equal to *antivirus* OR Plugin Name is equal to *anti-virus*) AND (Plugin Name is equal to *outdated* OR Plugin Name is equal to *signature*)
```

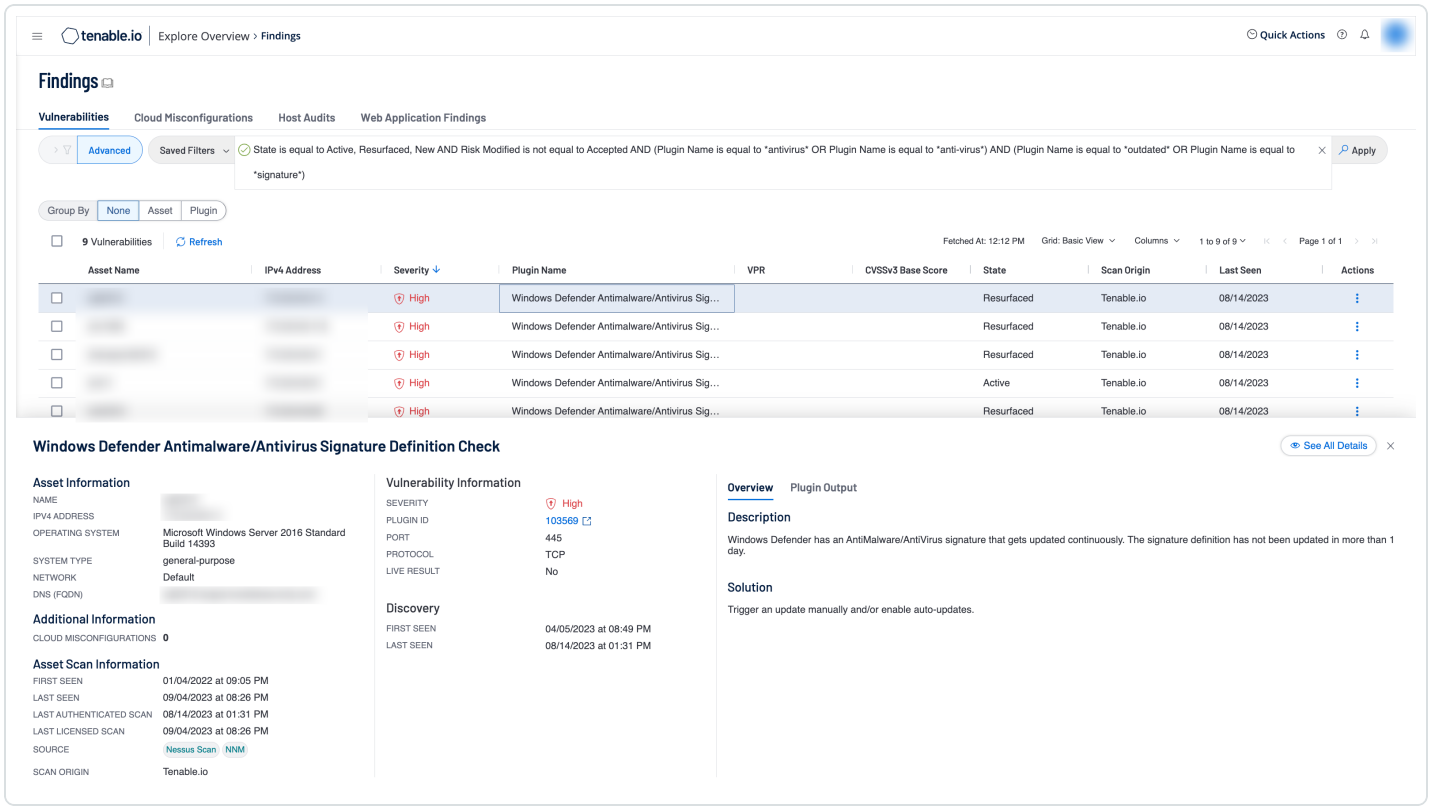
For the conditions stated above:

- State is set to Active, Resurfaced, and New, which eliminates any vulnerabilities that have been fixed.
- Risk Modified is not equal to Accepted, which eliminates all vulnerabilities that have previously been accepted.
- Plugin Name is equal to the text contained in Nessus plugins with the * being utilized as a wildcard. For example, *antivirus*, will match pluginID 16193 as the name contains the text.

Step 3: Click on the **Apply** button to begin the search.

This search detected output from Plugin ID [103569 Windows Defender Antimalware/Antivirus Signature Definition Check]

Step 4: Click on the Asset Name or Plugin Name to drill into further details about the malware exposure, as shown below.



Malware continues to evolve and grow more sophisticated both in attack methods and measures to evade security controls. Tenable solutions also evolve to help organizations quickly identify the presence of hostile software and the effectiveness of antivirus and malware controls.

Learn More

Tenable Resources

- Tenable Plugins Page
- Tenable Vulnerability Management Malware Defenses Dashboard
- Tenable Security Center Malware Defenses Dashboard

Compliance Resources

- - SI-3: Malicious Code Protection
- NIST Special Publication 800-171 Revision 2
  - 3.14.2: Provide protection from malicious code at designated locations within organizational systems
- NIST Special Publication 800-53 Revision 4
  - SI-3: Malicious Code Protection
- Center for Internet Security (CIS)
- CIS Control 10: Malware Defenses