



Tenable Cyber Exposure Study - Malware Defenses

Last Revised: September 26, 2023



Table of Contents

Overview	3
How Tenable Can Help	4
Keeping Anti-Malware Software Up-to-Date	7
Detecting Software Version	8
Detecting Out-of-Date Signatures	12
Learn More	15



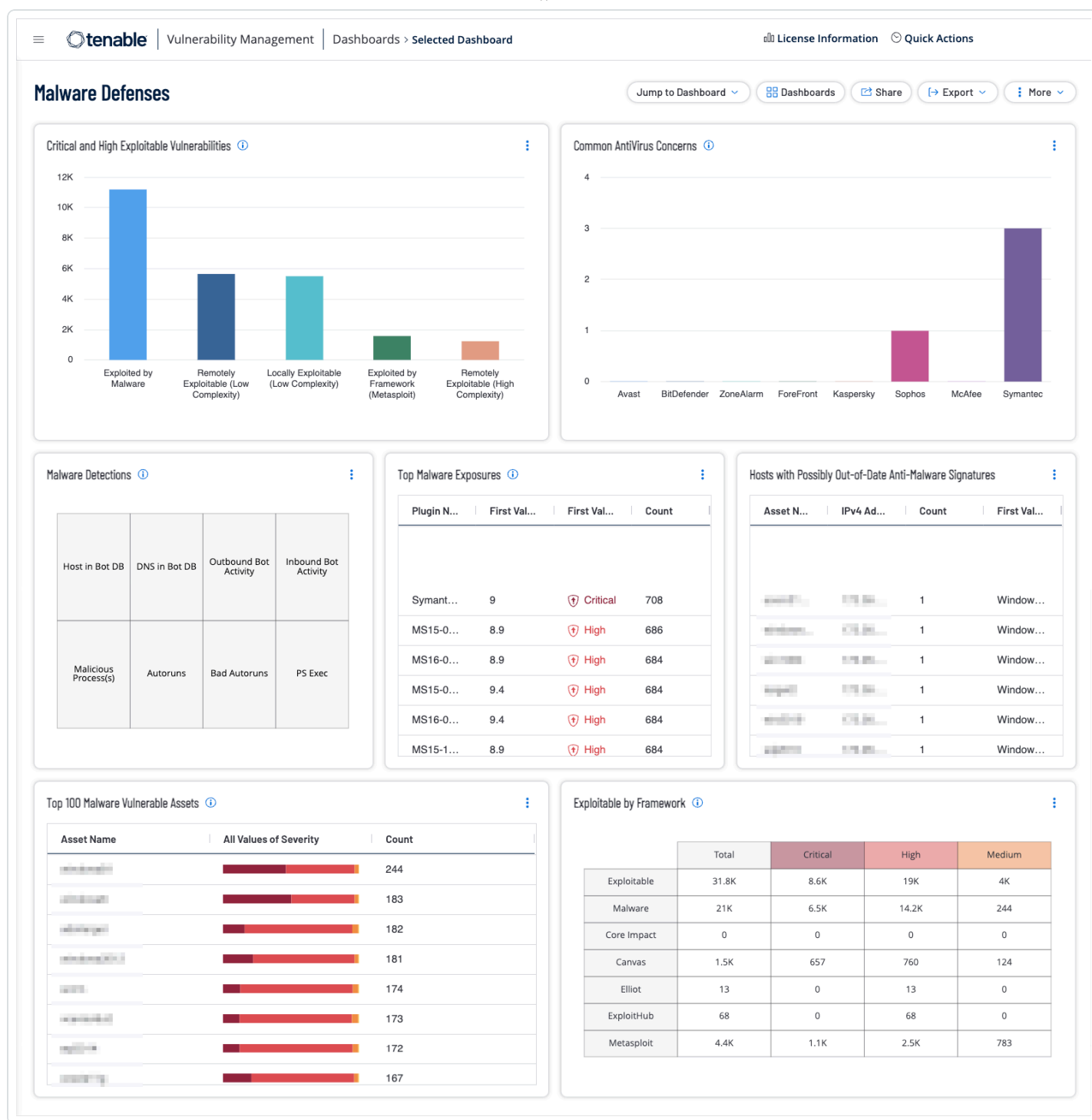
Overview

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.



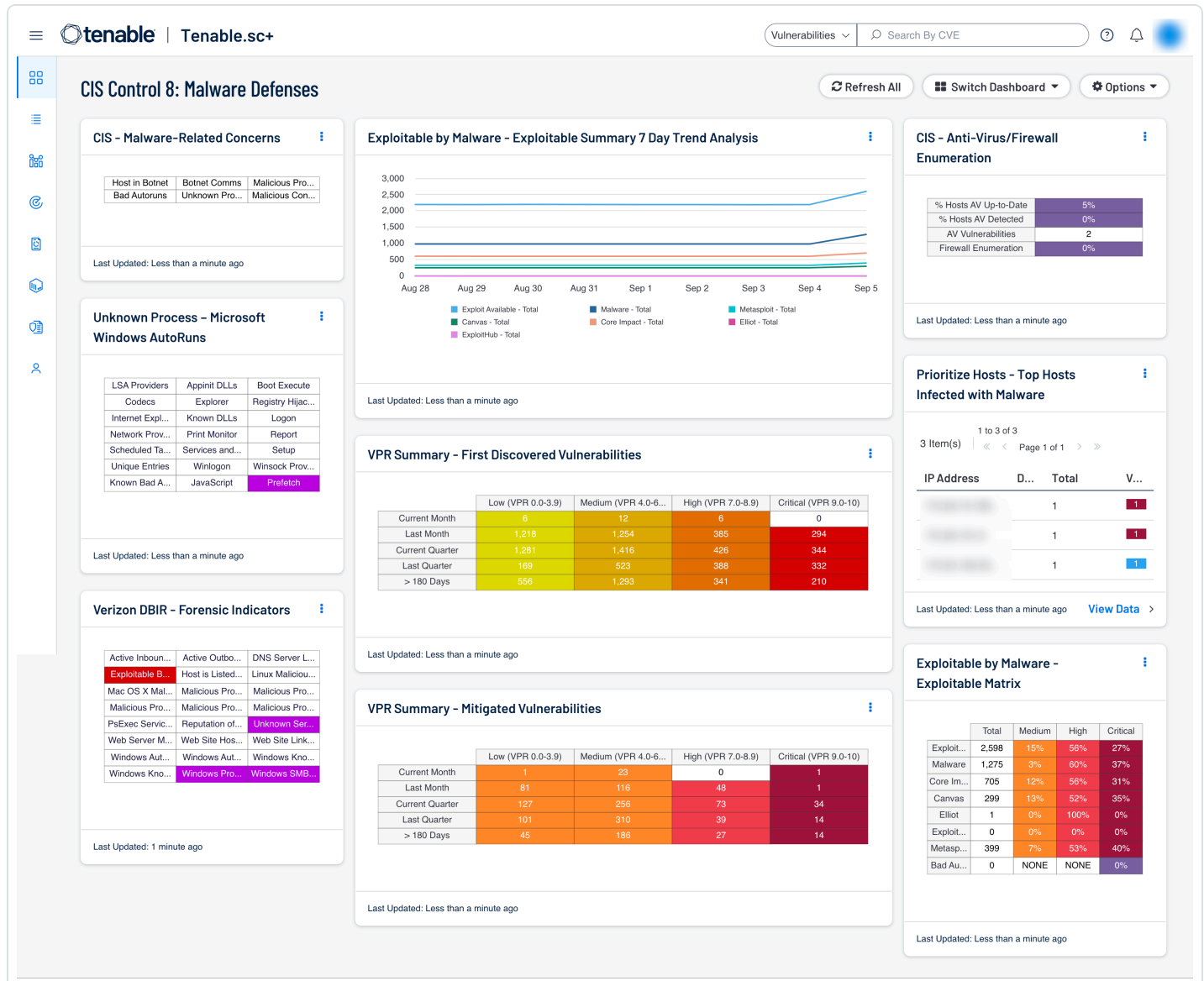
How Tenable Can Help

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

DETECTIONS

Plugins

Overview

Plugins Pipeline

Release Notes

Newest

Updated

Search

Nessus Families

WAS Families

NNM Families

LCE Families

Tenable OT Security Families

About Plugin Families

Audits

Policies

Indicators

ANALYTICS

CVEs

Attack Path Techniques

Plugins / Search

Plugins Search

Start typing or add a filter...

Filters (1)

CVSS v3 Base Score

Plugin Name (Active)

Clear All

Search by Plugin Name

antivirus

Page 1 of 2 • 64 Total

Next >>

ID	Name	Product	Family	Published	Updated	Severity
87777	Avast Antivirus Detection and Status	Nessus	Windows	1/7/2016	7/17/2023	CRITICAL
24232	BitDefender Antivirus Detection and Status	Nessus	Windows	1/22/2007	10/10/2022	CRITICAL
21725	Symantec Antivirus Software Detection and Status	Nessus	Windows	6/16/2006	10/10/2022	CRITICAL
21608	NOD32 Antivirus Detection and Status	Nessus	Windows	5/27/2006	2/6/2023	CRITICAL
20283	Panda Antivirus Detection and Status	Nessus	Windows	12/9/2005	2/6/2023	CRITICAL
16192	Trend Micro Antivirus Detection and Status	Nessus	Windows	1/18/2005	2/6/2023	CRITICAL
12107	McAfee Antivirus Detection and Status	Nessus	Windows	3/16/2004	10/10/2022	CRITICAL

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.

tenable.io | Explore Overview > Findings

Quick Actions

Findings

Vulnerabilities

Cloud Misconfigurations

Host Audits

Web Application Findings

Advanced

Saved Filters

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")

Apply

Group By

None

Asset

Plugin

27 Vulnerabilities

Refresh

Fetch At: 02:15 PM

Grid: Basic View

Columns

1 to 27 of 27

Page 1 of 1

Asset Name	IPv4 Address	Severity	Plugin Name	VPR	CVSSv3 Base Score	State	Scan Origin	Last Seen	Actions
		Critical	Sophos Anti-Virus Detection and Status (Linux)		10	Active	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Active	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		Info	Antivirus Software Check			Resurfaced	Tenable.io	08/14/2023	
		Info	Antivirus Software Check			Active	Tenable.io	08/14/2023	
		Info	Sophos Anti-Virus Installed (Linux)			Active	Tenable.io	08/14/2023	
		Info	Antivirus Software Check			Active	Tenable.io	08/14/2023	
		Info	Antivirus Software Check			Resurfaced	Tenable.io	08/14/2023	
		Info	Antivirus Software Check			New	Tenable.io	07/27/2022	
		Info	Antivirus Software Check			Active	Tenable.io	08/14/2023	
		Info	Antivirus Software Check			Active	Tenable.io	08/14/2023	



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**.

The screenshot shows the Tenable.io Findings page. At the top, there's a search bar with the 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')". Below the search bar, there's a table of findings. The first finding is highlighted with a red box and a red arrow labeled '1'. This finding is for the asset 'solaris11' with the plugin 'Sophos Anti-Virus Detection and Status (Linux)' and a severity of 'Critical'. Below the table, there's a detailed view of this finding. The detailed view is divided into three sections: 'Asset Information', 'Vulnerability Information', and 'Overview'. The 'Asset Information' section shows details about the asset 'solaris11'. The 'Vulnerability Information' section shows details about the vulnerability, including its severity, plugin ID, exploitability, protocol, CVSSv3 vector, CVSSv2 base score, CVSSv2 vector, live result, and discovery. The 'Overview' section shows the description and solution for the vulnerability. A red arrow labeled '2' points to the 'See All Details' button in the top right corner of the detailed view.

Asset Name	IPV4 Address	Severity	Plugin Name	VPR	CVSSv3 Base Score	State	Scan Origin	Last Seen	Actions
solaris11	172.26.48.100	Critical	Sophos Anti-Virus Detection and Status (Linux)		10	Active	Tenable.io	08/14/2023	
sql2016	172.26.48.14	High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
win1064	172.26.48.118	High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
sharepoint2019	172.26.48.41	High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
win11	172.26.48.31	High	Windows Defender Antimalware/Antivirus Sig...			Active	Tenable.io	08/14/2023	
win2019	172.26.48.38	High	Windows Defender Antimalware/Antivirus Sin...			Resurfaced	Tenable.io	08/14/2023	

Sophos Anti-Virus Detection and Status (Linux)

Asset Information

NAME: solaris11
IPV4 ADDRESS: 172.26.48.100
OPERATING SYSTEM: Solaris 11 (386)
SYSTEM TYPE: general-purpose
NETWORK: Default
DNS (FQDN):

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

Vulnerability Information

SEVERITY: Critical
PLUGIN ID: 133963
EXPLOITABILITY: @ >
PROTOCOL: TCP
CVSSv3 VECTOR: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S: C/C:H/I/H/A/H
CVSSv2 BASE SCORE: 10
CVSSv2 VECTOR: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
LIVE RESULT: No

Discovery

FIRST SEEN: 03/08/2023 at 10:01 PM
LAST SEEN: 08/14/2023 at 01:31 PM

Overview Plugin Output

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 All Details](#)

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.



[← Back to Findings](#)

Sophos Anti-Virus Detection and Status (Linux)

VULNERABILITIES **CRITICAL** PLUGIN ID 133963

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/>

[Previous](#) [Next](#) [Actions](#) ⌵

Asset Criticality Rating (ACR) ⓘ

Medium
4

Tenable-Provided
[More](#)

Finding State ⓘ

Active

Vulnerability Information

SEVERITY	Critical
EXPLOITABILITY	@ D
CPE	cpe:/a:sophos:sophos_antivirus
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 Affected

[VIEW ASSET DETAILS](#)

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 cpe:/a:sophos:smn - scanner:2.4.5.1

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:

The screenshot shows the Tenable Plugins Search interface. The search bar contains the text "signature antivirus". A red arrow points to the search bar. The results table shows several plugins, including "Windows Defender Antimalware/Antivirus Signature Definition Check" with ID 103569 and a "HIGH" severity level.

ID	Name	Product	Family	Published	Updated	Severity
103569	Windows Defender Antimalware/Antivirus Signature Definition Check	Nessus	Windows	10/2/2017	10/16/2020	HIGH
16193	Antivirus Software Check	Nessus	Windows	1/18/2005	2/1/2022	INFO
45051	WMI Antivirus Enumeration	Nessus	Windows	3/12/2010	7/17/2023	INFO
12107	McAfee Antivirus Detection and Status	Nessus	Windows	3/16/2004	10/10/2022	CRITICAL
31857	Symantec AntiVirus Scan Engine Detection	Nessus	Windows	4/14/2008	10/10/2022	INFO
64451	Mobile Signature Error	Nessus	Mobile Devices	2/4/2013	6/20/2023	INFO

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.

The screenshot shows the Tenable.io interface for the Findings page. The 'Findings' tab is selected. Below it, the 'Advanced' filter is active, showing a complex search query: "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*)". The results table shows 9 vulnerabilities, all with a severity of 'High' and a state of 'Resurfaced' or 'Active'. The 'Plugin Name' column is highlighted with a red arrow.

Asset Name	IPv4 Address	Severity	Plugin Name	VPR	CVSSv3 Base Score	State	Scan Origin	Last Seen	Actions
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Active	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	
		High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	

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.

Findings

Vulnerabilities Cloud Misconfigurations Host Audits Web Application Findings

Advanced Saved Filters 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") Apply

Group By None Asset Plugin

9 Vulnerabilities Refresh

Fetches At: 12:12 PM Grid: Basic View Columns 1 to 9 of 9 Page 1 of 1

Asset Name	IPv4 Address	Severity	Plugin Name	VPR	CVSSv3 Base Score	State	Scan Origin	Last Seen	Actions
[Redacted]	[Redacted]	High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	[More]
[Redacted]	[Redacted]	High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	[More]
[Redacted]	[Redacted]	High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	[More]
[Redacted]	[Redacted]	High	Windows Defender Antimalware/Antivirus Sig...			Active	Tenable.io	08/14/2023	[More]
[Redacted]	[Redacted]	High	Windows Defender Antimalware/Antivirus Sig...			Resurfaced	Tenable.io	08/14/2023	[More]

Windows Defender Antimalware/Antivirus Signature Definition Check See All Details

Asset Information

NAME [Redacted]
IPV4 ADDRESS [Redacted]
OPERATING SYSTEM Microsoft Windows Server 2016 Standard Build 14393
SYSTEM TYPE general-purpose
NETWORK Default
DNS (FQDN) [Redacted]

Additional Information

CLOUD MISCONFIGURATIONS 0

Asset Scan Information

FIRST SEEN 01/04/2022 at 09:05 PM
LAST SEEN 09/04/2023 at 08:26 PM
LAST AUTHENTICATED SCAN 08/14/2023 at 01:31 PM
LAST LICENSED SCAN 09/04/2023 at 08:26 PM
SOURCE Nessus Scan NNM
SCAN ORIGIN Tenable.io

Vulnerability Information

SEVERITY High
PLUGIN ID 103569
PORT 445
PROTOCOL TCP
LIVE RESULT No

Discovery

FIRST SEEN 04/05/2023 at 08:49 PM
LAST SEEN 08/14/2023 at 01:31 PM

Overview Plugin Output

Description

Windows Defender has an AntiMalware/AntiVirus signature that gets updated continuously. The signature definition has not been updated in more than 1 day.

Solution

Trigger an update manually and/or enable auto-updates.

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](#)