



# **Tenable Cyber Exposure Study - Email and Web Browser Security**

---

Last Revised: November 14, 2023

# Table of Contents

- How Tenable Can Help ..... 3**
- Ensure the Use of Only Fully Supported Email and Browser Clients ..... 3**
- Drilling Down in Tenable Vulnerability Management ..... 4**
- Drilling Down in Tenable Security Center ..... 6**
  - Further Identification of Web Browsers and Email Applications in Tenable Vulnerability Management ..... 8
  - Further Identification of Web Browsers and Email Applications in Tenable Security Center .. 9
  - Restrict Unnecessary or Unauthorized Browser and Email Client Extensions .....10
  - Anti-Malware Protections .....13
  - Utilizing Audit Files .....14
- Learn More ..... 18**

## How Tenable Can Help

---

Everyone uses email and web browsers to communicate and access a wide variety of systems from commercial sites to enterprise systems. Email and web browser applications represent two of the most essential tools for communication and information access. Vulnerabilities are a common concern and these applications are prime targets for cyber attacks.

The Center for Internet Security (CIS) states:

*"Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering."*

Clicking on malware designed to deceive users, either inside of an email or on a malicious website, is certainly a very common and successful method of attack. However, this method is best cured with a solid cybersecurity awareness program. Security training is an invaluable tool in educating users on best practices; in particular on how to identify phishing emails, how to avoid browser plugins, extensions, and keeping applications up-to-date. All of which reduce the likelihood of this type of attack being successful.

Another common attack path is via unpatched applications. Email clients and web browsers which are unpatched, may contain vulnerabilities that allow a compromised user's device to be vulnerable to a number of attacks. In regard to web browsers, malicious or poorly coded extensions may allow attackers to gain unauthorized access to sensitive information, or inject malicious code.

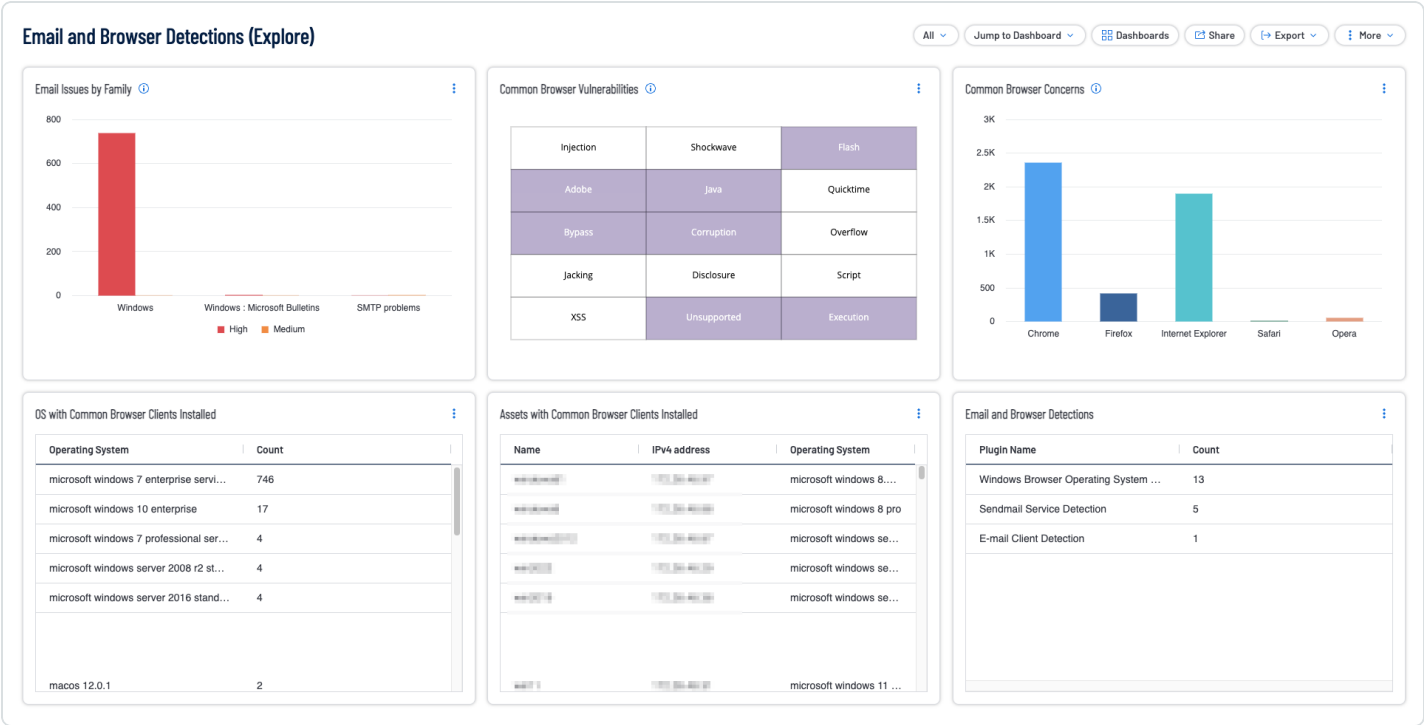
To mitigate these vulnerabilities, users and organizations should practice safe email and web browsing habits, keep software up-to-date, and utilize anti-virus and anti-phishing software. Tenable can assist organizations to reduce these threats by minimizing the attack surface associated with web browsers and email systems.

## Ensure the Use of Only Fully Supported Email and Browser Clients

---

Tenable products allow security operation teams to use Tenable One to analyze endpoint browser and email client configurations. Using a variety of active and passive plugins paired with Tenable

Vulnerability Management, the organization can verify that established configuration policies are followed. Tenable provides several solutions for organizations to better understand vulnerability management. As an example, the Tenable Nessus Network Monitor can passively detect and enumerate web browsers that are being utilized, as well as any potential vulnerabilities present in the versions detected. Active, credentialed, scanning by Tenable Nessus can provide detailed information on web browsers that are installed via the same methods of software enumeration described in the relevant CIS Controls. Analysts can easily produce tables and matrices utilizing this information, for a variety of browser clients such as Chrome, Firefox, Internet Explorer, Safari, and more, which are part of the **Email and Browser Detections Dashboard** for Tenable Vulnerability Management, as shown in the following image:



## Drilling Down in Tenable Vulnerability Management

Clicking on an item, in this case, **Common Browser Concerns, Chrome** bar, takes you to the **Findings** page. Clicking on one of the items brings up a summary from the bottom of the page.

## Findings

Vulnerabilities
Cloud Misconfigurations
Host Audits
Web Application Findings

Advanced
Saved Filters
Plugin Name is equal to "chrome" AND CPE is not equal to cpe:/o AND Severity is equal to Medium, High, Critical AND Risk Modified is not equal to Accepted AND State is equal to Active, Resurfaced, New
Apply

Group By
None
Asset
Plugin

16,313 Vulnerabilities
Refresh

Asset Name	IPV4 Address	Severity	Plugin Name	VPR	CVSSv3 Base ...	State	Scan Origin	Asset Tags	Last Seen	Actions
		Critical	Google Chrome < 94.0.4606.71 Multi...	6.7		New	Tenable.io		10/20/2022	
		Critical	Google Chrome < 97.0.4692.71 Multi...	6.7		New	Tenable.io		10/20/2022	
		Critical	Google Chrome < 99.0.4844.51 Multi...	6.7		New	Tenable.io		10/20/2022	
		Critical	Google Chrome < 95.0.4638.54 Multi...	7.3		New	Tenable.io		10/20/2022	
		Critical	Google Chrome < 90.0.4430.72 Multi...	6.5		New	Tenable.io		10/20/2022	

### Google Chrome < 94.0.4606.71 Multiple Vulnerabilities

#### Asset Information

NAME

IPV4 ADDRESS

OPERATING SYSTEM

SYSTEM TYPE

NETWORK

Additional Information

CLOUD MISCONFIGURATIONS

#### Asset Scan Information

FIRST SEEN

LAST SEEN

LAST LICENSED SCAN

SOURCE

SCAN ORIGIN

#### Vulnerability Information

SEVERITY

PLUGIN ID

PATCH PUBLISHED

PORT

PROTOCOL

CVSSV2 VECTOR

#### Discovery

FIRST SEEN

LAST SEEN

#### VPR Key Drivers

VPR SCORE

THREAT INTENSITY

#### Overview

##### Description

The version of Google Chrome installed on the remote host is prior to 94.0.4606.71. It is, therefore, affected by multiple vulnerabilities as referenced in the 2021\_09\_stable-channel-update-for-desktop\_30 advisory. Note that Nessus Network Monitor has not tested for this issue but has instead relied only on the application's self-reported version number.

##### Solution

Upgrade to Google Chrome version 94.0.4606.71 or later.

See All Details

Clicking on **See All Details** opens the **Details** page. The details page provides a wealth of information, including the description, solution, asset details, and key findings on the right side of the page, as shown in the following image:

Back to Findings

## Google Chrome < 94.0.4606.71 Multiple Vulnerabilities

VULNERABILITIES
CRITICAL
PLUGIN ID 701369

### Description

The version of Google Chrome installed on the remote host is prior to 94.0.4606.71. It is, therefore, affected by multiple vulnerabilities as referenced in the 2021\_09\_stable-channel-update-for-desktop\_30 advisory. Note that Nessus Network Monitor has not tested for this issue but has instead relied only on the application's self-reported version number.

### Solution

Upgrade to Google Chrome version 94.0.4606.71 or later.

### See Also

None

### Asset Affected

View Asset Details

#### Asset Information

ASSET ID

NAME

IPV4 ADDRESS

OPERATING SYSTEM

SYSTEM TYPE

PUBLIC

#### Additional Information

CLOUD MISCONFIGURATIONS

#### Asset Scan Information

FIRST SEEN

LAST SEEN

LAST LICENSED SCAN

SOURCE

SCAN ORIGIN

#### Additional Information

NETWORK

MAC ADDRESS

#### Plugin Output

The observed version of Google Chrome is: 85.0.4158.0

### Vulnerability Priority Rating (VPR)

6.7

### Finding State

New

### Vulnerability Information

SEVERITY

VULN PUBLISHED

EXPLOITABILITY

PATCH PUBLISHED

PORT

PROTOCOL

### Discovery

FIRST SEEN

LAST SEEN

AGE

### VPR Key Drivers

THREAT INTENSITY

EXPLOIT CODE MATURITY

AGE OF VULN

PRODUCT COVERAGE

CVSS3 IMPACT SCORE

THREAT SOURCES

### Plugin Details

For each browser, a matrix displays warning indicators for detected vulnerabilities, including critical vulnerabilities, vulnerabilities known to be exploitable, vulnerabilities by product used in conjunction with the browser (such as Flash or Java), and vulnerabilities by keyword. The keywords cover the major web browser threats such as memory corruption, information disclosure, remote code execution, buffer overflows, cross-site scripting (XSS), and more.

## Drilling Down in Tenable Security Center

Clicking on a cell, in this case, the **Browser Vulnerabilities - Summary by Browser, Chrome** row (either **Vulnerabilities** or **Systems**) takes you to the **Vulnerability Analysis** page. Clicking on the **Go to Vulnerability Details** presents you with the **Vulnerability Details** page which contains a significant amount of information related to the particular vulnerability.

[IP Summary](#) > [Vulnerability Detail List](#)

## Vulnerability Detail List

[Options](#)

[Vulnerabilities](#) [Web App Scanning](#) [Queries](#) [Events](#) [Mobile](#)

Apply

+ Customize

✕ Clear All

Load Query

▼ Plugin Family

# ▼

Search

Q

☐ Select All

☒ Operating System Detectio...

☐ Abuse [Passive]

☐ AIX Local Security Checks

☐ Alma Linux Local Security ...

▼ Plugin Name

Contains ▼

chrome

> Address

Google Chrome Detection (Windows)(34196)

VULNERABILITY

INFO

[Launch Remediation Scan](#)

[Accept Risk](#)

[Recast Risk](#)

< Result 1 of 9,409 >

### Synopsis

The remote Windows host contains a web browser.

### Description

Google Chrome, a web browser from Google, is installed on the remote Windows host.

### See Also

LINKS:

[google.com](#)

### Output

Path : C:\Program Files (x86)\Google\Chrome\Application

Version : 110.0.5481.104

Copy

Note that Nessus only looked in the registry for evidence of Google Chrome. If there are multiple users on this host, you may wish to enable the 'Perform thorough tests' setting and re-scan. This will cause Nessus to scan each local user's directory for installs.

### Discovery

FIRST DISCOVERED: 4 months ago

LAST OBSERVED: 4 months ago

### Host Information

### Risk Information

CVSS V2 SEVERITY: None

### Exploit Information

EXPLOIT AVAILABLE: No

### Plugin Details

PLUGIN ID: 34196

PUBLISHED: Sep 12, 2008

LAST MODIFIED: Oct 10, 2022

FAMILY: Windows

VERSION: 1.26

TYPE: local

### Vulnerability Information

CPE:

cpe:/a:google:chrome

### Reference Information

As discussed, reducing the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems is a critical effort. One of the most important aspects of this effort is the identification of installed web and email applications. Items on the dashboard display information on the most common applications. However, there are times when less common web or email applications are in use and must be identified.

# Further Identification of Web Browsers and Email Applications in Tenable Vulnerability Management

For example, If we wanted to identify endpoints which had Chrome installed, we could filter on **pluginID = 20811**, with a **Plugin Output = \*chrome\*** (asterisk specifies a wildcard element).

Begin by navigating to the **Findings** page and we would get results similar to the following screenshot, which shows results for all the hosts which have Chrome installed:

**Findings**

Vulnerabilities Cloud Misconfigurations Host Audits Web Application Findings

Advanced Saved Filters Plugin ID is equal to 20811 AND Plugin Output contains \*chrome\* Apply

Group By None Asset Plugin

7 Vulnerabilities Refresh

Fetch At: 11:56 AM Grid: Basic View Columns 1 to 7 of 7 Page 1 of 1

Asset Name	IPv4 Address	Seve...	Plugin Name	VPR	CVSSv...	State	Scan Origin	Last Seen	Actions
		Info	Microsoft Windows Installed Software Enumeration...			Active	Tenable.io	09/21/2023	
		Info	Microsoft Windows Installed Software Enumeration...			Active	Tenable.io	09/21/2023	
		Info	Microsoft Windows Installed Software Enumeration...			Resurfac...	Tenable.io	09/21/2023	
		Info	Microsoft Windows Installed Software Enumeration...			Active	Tenable.io	09/21/2023	
		Info	Microsoft Windows Installed Software Enumeration...			Resurfac...	Tenable.io	09/21/2023	
		Info	Microsoft Windows Installed Software Enumeration...			Resurfac...	Tenable.io	09/21/2023	
		Info	Microsoft Windows Installed Software Enumeration...			Active	Tenable.io	09/21/2023	

[Back to Findings](#)

## Microsoft Windows Installed Software Enumeration (credentialed check)

VULNERABILITIES INFO PLUGIN ID 20811

**Description**

This plugin lists software potentially installed on the remote host by crawling the registry entries in :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall  
HKLM\SOFTWARE\Microsoft\Updates  
[More](#)

**Solution**

Remove any applications that are not compliant with your organization's acceptable use and security policies.

**See Also**

None

**Asset Affected** [View Asset Details](#)

**Asset Information**

ASSET ID [redacted]

NAME [redacted]

IPV4 ADDRESS [redacted]

OPERATING SYSTEM Microsoft Windows Server 2012 R2 Standard Build 9600

SYSTEM TYPE general-purpose

PUBLIC No

**Additional Information**

**Plugin Output**

The following software are installed on the remote host :

AutoIt v3.3.14.5 [version 3.3.14.5]  
Google Chrome [version 109.0.5414.165] [installed on 2023/09/13]  
Notepad++ (32-bit x86) [version 7.6]  
WizTree v3.30 [version 3.30] [installed on 2019/11/22]  
WinSCP 5.17.7 [version 5.17.7] [installed on 2020/09/20]  
Microsoft Visual C++ 2005 Redistributable (x64) [version 8.0.56336] [installed on 2018/02/07]  
Microsoft Visual C++ 2022 X64 Minimum Runtime - 14.32.31332 [version 14.32.31332] [installed on 2023/08/07]  
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.32.31332 [version 14.32.31332.0]

**Asset Criticality Rating (ACR)**

High 8

Tenable-Provided [More](#)

**Finding State**

Active

**Vulnerability Information**

SEVERITY Info

ASSET INVENTORY True

PORT 445

PROTOCOL TCP

LIVE RESULT No

**Discovery**

FIRST SEEN 02/21/2023 at 05:46 AM

LAST SEEN 09/21/2023 at 05:50 AM

AGE 220 Days



# Further Identification of Web Browsers and Email Applications in Tenable Security Center

For Tenable Security Center, the process is similar. From the Analysis tab, filter on **pluginID = 20811 (1)**, with a **Vulnerability Text contains chrome (2)** (REGEX can also be used if REGEX is selected in lieu of "Contains" from the dropdown) and we would get results similar to the screenshot below, which shows results for all the hosts which have Chrome installed.

The screenshot displays the 'Vulnerability Detail List' for the plugin 'Microsoft Windows Installed Software Enumeration (credentialed check) (20811)'. The interface includes a left sidebar with navigation options and a main content area with details and filters.

**Filters:**

- Plugin ID:** 20811
- Vulnerability Text:** Contains chrome

**Details:**

- Synopsis:** It is possible to enumerate installed software.
- Description:** This plugin lists software potentially installed on the remote host by crawling the registry entries in: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall, HKLM\SOFTWARE\Microsoft\Updates. Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.
- Steps to Remediate:** Remove any applications that are not compliant with your organization's acceptable use and security policies.
- Output:** The following software are installed on the remote host :
  - Google Chrome [version 110.0.5481.104] [installed on 2023/02/16]
  - HP Device Manager Console [version 5.0.3610.39629] [installed on 2022/08/31]
  - HP Device Manager Console Web Bridge [version 5.0.3700.39541] [installed on 2022/08/31]
  - HP Device Manager Gateway [version 5.0.3630.39510] [installed on 2022/08/31]
  - HP Device Manager HTTPS Repository [version 5.0.3690.39631] [installed on 2022/08/31]

**Discovery:** FIRST DISCOVERED: 4 months ago, LAST OBSERVED: 4 months ago

**Host Information:** [Redacted]

**Risk Information:** CVSS V2 SEVERITY: None

**Exploit Information:** EXPLOIT AVAILABLE: No

**Plugin Details:** PLUGIN ID: 20811, PUBLISHED: Jan 26, 2006, LAST MODIFIED: Feb 1, 2022, FAMILY: Windows, VERSION: 1.21, TYPE: local

**Reference Information:** CROSS REFERENCES: IAVT:0001-T-0501

The plugin output contains the version of Google Chrome and the date the application was installed. Additional searches can be performed using specific application version searches if so desired. Filters created here to refine search results, can also be used to refine vulnerability results displayed within components.

# Restrict Unnecessary or Unauthorized Browser and Email Client Extensions

---

Organizations need to determine which browser extensions are authorized, and which ones are not. Once this determination is made, restrict either through uninstalling or disabling any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

There are Tenable Nessus plugins, which detect or enumerate extensions, such as plugin **96533 - Chrome Browser Extension Enumeration** and **133180 Chrome Browser Extension Enumeration (macOS)**. If the proper credentials are utilized, these plugins will enumerate Chrome extensions for all users.

In both of the examples below (Tenable Vulnerability Management and Tenable Security Center), the plugin output contains information regarding the:

- User who has the extension installed
- The Name of the Extension
- The Version of the Extension
- The date of the Last Update
- The installation Path

This allows analysts reviewing the information and the administrator or operational staff to have the most complete and reliable information needed to take corrective action.

Vulnerability Summary > Vulnerability Detail List

## Vulnerability Detail List

Vulnerabilities Web App Scanning Queries Events Mobile

Apply

+ Customize x Clear All

Load Query

Plugin ID

20811

Vulnerability Text

Contains

chrome

### Microsoft Windows Installed Software Enumeration (credentialed check)(20811)

VULNERABILITY INFO

Launch Remediation Scan Accept Risk Recast Risk

Result 1 of 1,120

#### Synopsis

It is possible to enumerate installed software.

#### Description

This plugin lists software potentially installed on the remote host by crawling the registry entries in:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
HKLM\SOFTWARE\Microsoft\Updates
```

Note that these entries do not necessarily mean the applications are actually installed on the remote host - they may have been left behind by uninstallers, or the associated files may have been manually removed.

#### Steps to Remediate

Remove any applications that are not compliant with your organization's acceptable use and security policies.

#### Output

The following software are installed on the remote host :

```
Google Chrome [version 110.0.5481.104] [installed on 2023/02/16]
HP Device Manager Configuration Center [version 5.0.3700.39541] [installed on 2022/08/31]
HP Device Manager Console [version 5.0.3610.39629] [installed on 2022/08/31]
HP Device Manager Console Web Bridge [version 5.0.3700.39541] [installed on 2022/08/31]
HP Device Manager Gateway [version 5.0.3630.39510] [installed on 2022/08/31]
HP Device Manager HTTPS Repository [version 5.0.3690.39631] [installed on 2022/08/31]
```

Copy

#### Discovery

FIRST DISCOVERED: 4 months ago  
LAST OBSERVED: 4 months ago

#### Host Information

IP ADDRESS: 10.10.10.10  
HOSTNAME: 10.10.10.10  
OS: Windows  
OS VERSION: 10.0.19041.1  
OS ARCHITECTURE: x64

#### Risk Information

CVSS V2 SEVERITY: None

#### Exploit Information

EXPLOIT AVAILABLE: No

#### Plugin Details

PLUGIN ID: 20811  
PUBLISHED: Jan 26, 2006  
LAST MODIFIED: Feb 1, 2022  
FAMILY: Windows  
VERSION: 1.21  
TYPE: local

#### Reference Information

CROSS REFERENCES: IAVT0001-T-0501

The plugin output contains the version of Google Chrome and the date the application was installed. Additional searches can be performed using specific application version searches if so desired. Filters created here to refine search results, can also be used to refine vulnerability results displayed within components.

## Tenable Vulnerability Management

← Back to Findings

Chrome Browser Extension Enumeration

VULNERABILITIES INFO PLUGIN ID 96533

Description

Nessus was able to enumerate Chrome browser extensions installed on the remote host.

Solution

Make sure that the use and configuration of these extensions comply with your organization's acceptable use and security policies.

See Also

<https://chrome.google.com/webstore/category/extensions>

Previous

Next

Actions

Asset Criticality Rating (ACR)

Medium

4

Tenable-Provided

More

Finding State

Resurfaced

Vulnerability Information

SEVERITY

PORT

PROTOCOL

LIVE RESULT

Info

445

TCP

No

Discovery

FIRST SEEN

LAST SEEN

AGE

10/21/2019 at 04:10 AM

10/26/2023 at 05:01 PM

1467 Days

Plugin Details

PUBLICATION DATE

MODIFICATION DATE

FAMILY

TYPE

VERSION

PLUGIN ID

01/16/2017

10/09/2023

Windows

Local

1.199

96533

Risk Information

RISK FACTOR

Info

Asset Affected

View Asset Details

Asset Information

ASSET ID

NAME

IPV4 ADDRESS

OPERATING SYSTEM

SYSTEM TYPE

PUBLIC

Microsoft Windows 10 Pro Build 19041

Microsoft Windows 10 Pro

general-purpose

No

Additional Information

CLOUD MISCONFIGURATIONS

Asset Scan Information

FIRST SEEN

LAST SEEN

LAST AUTHENTICATED SCAN

LAST LICENSED SCAN

SOURCE

SCAN ORIGIN

05/31/2017 at 11:30 AM

10/26/2023 at 05:01 PM

10/26/2023 at 05:01 PM

10/26/2023 at 05:01 PM

Nessus Scan

Tenable.io

Additional Information

Cloud Misconfigurations

Plugin Output

Copy

User : Administrator  
|- Browser : Chrome  
|- Add-on information :  
  
Name : Google Docs Offline  
Description : Edit, create, and view your documents, spreadsheets, and presentations – all without internet access.  
Version : 1.66.0  
Update Date : Oct. 23, 2023 at 06:34:01 GMT  
Path : C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpdloisfmeeakhlbnhnqdjjljjlll\1.66.0\_0  
  
Name : Chrome Web Store Payments  
Description : Chrome Web Store Payments  
Version : 1.0.0.6  
Update Date : Oct. 23, 2023 at 06:34:02 GMT  
Path : C:\Users\Administrator\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpicmgmieda\1.0.0.6\_0

## Tenable Security Center

Vulnerability Summary > Vulnerability Detail List

Vulnerability Detail List

Vulnerabilities Web App Scanning Queries Events Mobile

Apply

Customize Clear All

Load Query

Plugin ID

96533

Chrome Browser Extension Enumeration (96533)

VULNERABILITY INFO

Launch Remediation Scan Accept Risk Recast Risk

Synopsis

One or more Chrome browser extensions are installed on the remote host.

Description

Nessus was able to enumerate Chrome browser extensions installed on the remote host.

Steps to Remediate

Make sure that the use and configuration of these extensions comply with your organization's acceptable use and security policies.

See Also

LINKS:

google.com

Output

User : admin  
|- Browser : Chrome  
|- Add-on information :  
  
Name : Google Docs Offline  
Description : Edit, create, and view your documents, spreadsheets, and presentations – all without internet access.  
Version : 1.50.1  
Update Date : Feb. 17, 2023 at 18:29:36 GMT  
Path : C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extensions\ghbmnnjooekpdloisfmeeakhlbnhnqdjjljjlll\1.50.1\_0  
  
Name : Chrome Web Store Payments  
Description : Chrome Web Store Payments  
Version : 1.0.0.6  
Update Date : Feb. 17, 2023 at 18:29:36 GMT  
Path : C:\Users\admin\AppData\Local\Google\Chrome\User Data\Default\Extensions\nmmhkkegccagdldgiimedpicmgmieda\1.0.0.6\_0

Copy

Discovery

FIRST DISCOVERED: 4 months ago  
LAST OBSERVED: 4 months ago

Host Information

IP Address

Host Name

Operating System

Product

Version

10.10.10.10

10.10.10.10

Microsoft Windows 10 Pro

10.10.10.10

10.10.10.10

Risk Information

CVSS V2 SEVERITY: None

Exploit Information

EXPLOIT AVAILABLE: No

Plugin Details

PLUGIN ID

PUBLISHED

LAST MODIFIED

FAMILY

VERSION

TYPE

96533

Jan 16, 2017

Oct 9, 2023

Windows

1.199

local

Vulnerability Information

CPE:  
cpe:/a:google:chrome

Reference Information

CROSS REFERENCES: IAVT-0001-T-0511

# Anti-Malware Protections

---

Malicious software or “malware”, is software 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. 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.

For more information on malware detection, visit the [Malware Defenses Cyber Exposure Study](#).

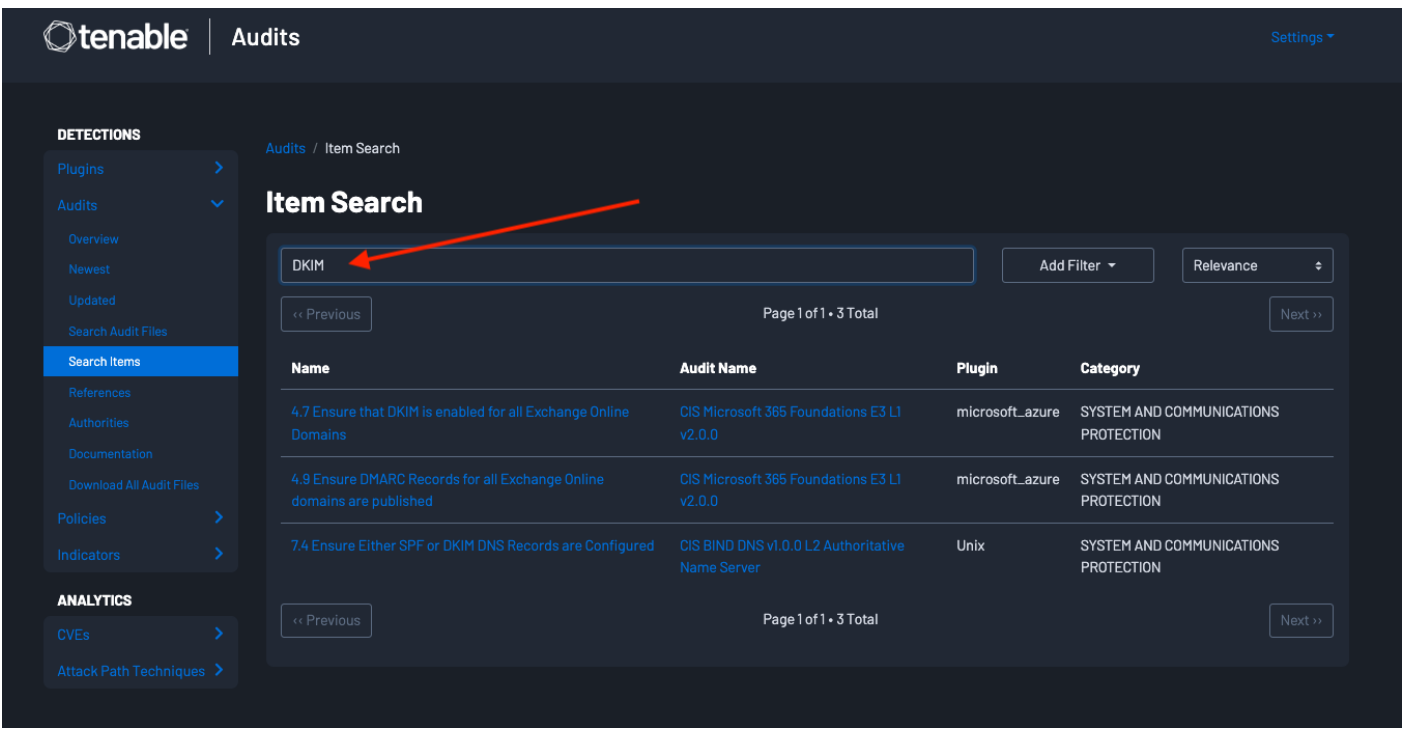
# Utilizing Audit Files

## DKIM and DMARC

DomainKeys Identified Mail (DKIM) is an authentication method which detects forged sender addresses in email. Forging signatures is a technique used in many phishing and email spam campaigns. DKIM allows the recipient to check the email signature and ensure the email came from the domain stated.

Domain Message Authentication Reporting (DMARC) is an email authentication policy and reporting protocol. DMARC builds onto SPF and DKIM protocols by adding linkage to the author ("From") domain. This improves the protection for fraudulent email.

Tenable has audit files for Microsoft (CIS Microsoft 365 Foundations E3 L1 v1.5.0) that check for SPF, DKIM, and DMARC records. Additionally, an audit file (CIS BIND DNS v1.0.0 L2 Authoritative Name Server) for Unix systems, containing checks to ensure Either SPF or DKIM DNS Records are configured, is available. These audit files may be downloaded and reviewed on the [Tenable Audits](#) page. Locating audit files for key terms, such as SPF, DKIM, DMARC, and other terms should be performed on the [Item Search](#) page. Once that page is accessed type the search term, **DKIM** in this example, into the search bar.



The screenshot displays the Tenable Audits interface. On the left, a sidebar contains navigation links under 'DETECTIONS' (Plugins, Audits, Overview, Newest, Updated, Search Audit Files, Search Items, References, Authorities, Documentation, Download All Audit Files, Policies, Indicators) and 'ANALYTICS' (CVEs, Attack Path Techniques). The main area is titled 'Audits / Item Search' and 'Item Search'. A search bar contains the text 'DKIM', with a red arrow pointing to it. To the right of the search bar are buttons for 'Add Filter' and 'Relevance'. Below the search bar, a table lists search results. The table has columns for Name, Audit Name, Plugin, and Category. The results are as follows:

Name	Audit Name	Plugin	Category
4.7 Ensure that DKIM is enabled for all Exchange Online Domains	CIS Microsoft 365 Foundations E3 L1 v2.0.0	microsoft_azure	SYSTEM AND COMMUNICATIONS PROTECTION
4.9 Ensure DMARC Records for all Exchange Online domains are published	CIS Microsoft 365 Foundations E3 L1 v2.0.0	microsoft_azure	SYSTEM AND COMMUNICATIONS PROTECTION
7.4 Ensure Either SPF or DKIM DNS Records are Configured	CIS BIND DNS v1.0.0 L2 Authoritative Name Server	Unix	SYSTEM AND COMMUNICATIONS PROTECTION

Navigation controls include '<< Previous', 'Page 1 of 1 • 3 Total', and 'Next >>'.

The results will be presented. From these results you can click on the Name. In this example, the first option is selected, **4.7 Ensure that DKIM is enabled for all Exchange Online Domains** and we are presented with detailed information regarding this audit check.

The screenshot displays the Tenable Audits interface. On the left, a sidebar contains navigation links for 'DETECTIONS' (Plugins, Audits, Overview, Newest, Updated, Search Audit Files, Search Items, References, Authorities, Documentation, Download All Audit Files) and 'ANALYTICS' (CVEs, Attack Path Techniques). The main content area is titled 'Audits' and shows a breadcrumb trail: 'Audits / Items / 4.7 Ensure that DKIM is enabled for all Exchange Online Domains'. The audit title is prominently displayed. Below the title, the 'Information' section explains DKIM and its use. The 'Rationale' section describes the impact of enabling DKIM. The 'Impact' section states that there should be no impact. A 'NOTE' indicates that Nessus has not performed this check. The 'Solution' section provides instructions on how to set up DKIM records. On the right, the 'Item Details' section lists the 'Audit Name', 'Category', 'References', 'Plugin', and 'Control ID'.

**4.7 Ensure that DKIM is enabled for all Exchange Online Domains**

**Information**

DKIM is one of the trio of Authentication methods (SPF, DKIM and DMARC) that help prevent attackers from sending messages that look like they come from your domain.

DKIM lets an organization add a digital signature to outbound email messages in the message header. When DKIM is configured, the organization authorizes its domain to associate, or sign, its name to an email message using cryptographic authentication. Email systems that get email from this domain can use a digital signature to help verify whether incoming email is legitimate.

Use of DKIM in addition to SPF and DMARC to help prevent malicious actors using spoofing techniques from sending messages that look like they are coming from your domain.

**Rationale:**

By enabling DKIM with Office 365, messages that are sent from Exchange Online will be cryptographically signed. This will allow the receiving email system to validate that the messages were generated by a server that the organization authorized and not being spoofed.

**Impact:**

There should be no impact of setting up DKIM however, organizations should ensure appropriate setup to ensure continuous mail-flow.

**NOTE:** Nessus has not performed this check. Please review the benchmark to ensure target compliance.

**Solution**

To setup DKIM records, first add the following records to your DNS system, for each domain in Exchange Online that you plan to use to send email with:

For each accepted domain in Exchange Online, two DNS entries are required.

**Item Details**

**Audit Name:** CIS Microsoft 365 Foundations E3 L1 v2.0.0

**Category:** SYSTEM AND COMMUNICATIONS PROTECTION

**References:** 800-53ISC-7, CSCv7I7.8

**Plugin:** microsoft\_azure

**Control ID:** d43a0b0c8d38b7b1b6336fdf3f9e06508ccea0b727faaf b95d3506a2ba771939 [Q](#)

Clicking on the Audit Name, in this example CIS Microsoft 365 Foundations E3 L1 v2.0.0, provides a description of the audit items, and a download button in the top right corner.

The screenshot displays the Tenable Audits interface. On the left, a sidebar contains navigation links under 'DETECTIONS' (Plugins, Audits, Overview, Newest, Updated, Search Audit Files, Search Items, References, Authorities, Documentation, Download All Audit Files) and 'ANALYTICS' (CVEs, Attack Path Techniques). The main content area is titled 'Audits / CIS Microsoft 365 Foundations E3 L1 v2.0.0'. Below this, the title 'CIS Microsoft 365 Foundations E3 L1 v2.0.0' is prominently displayed with a 'Download File' button. The interface is divided into two main sections: 'Audit Details' and 'File Details'. 'Audit Details' lists: Name: CIS Microsoft 365 Foundations E3 L1 v2.0.0, Updated: 10/6/2023, Authority: CIS, Plugin: microsoft\_azure, Revision: 1.0, and Estimated Item Count: 45. 'File Details' lists: Filename: CIS\_Microsoft\_365\_v2.0.0\_E3\_Level\_1.audit, Size: 121 kB, MD5: 17bcae4cf311ddb02a0690b29794967, and SHA256: 73e0bc4e34a5b328f3a00dd0e2d0aced318904d8831e1eac78c09b549bef6f33. Below these, the 'Audit Items' section is shown with tabs for 'Items' and 'Changelog'. It contains a table with three items:

Description	Categories
1.1.1 Ensure Security Defaults is disabled on Azure Active Directory	CONFIGURATION MANAGEMENT
1.1.2 Ensure multifactor authentication is enabled for all users in administrative roles	IDENTIFICATION AND AUTHENTICATION
1.1.3 Ensure Sign-in frequency is enabled and browser sessions are not persistent for Administrative users	ACCESS CONTROL

For information related to adding an audit file to Tenable Security Center, refer to the [Audit File](#) section of the Tenable documentation site.

For information related to utilizing audit files in Tenable Vulnerability Management, refer to the [Compliance in Tenable Vulnerability Management Scans](#) section of the Tenable documentation site.

For detailed information on utilizing audit files and credentialed scanning information, review the [Tenable Compliance Checks Reference Guide](#).

In most environments which use the Microsoft Office system, Outlook is often already the default program for email, contacts, and calendaring. Compliance checks exist to ensure group policies are set to make Outlook the default program for email. Installed web browsers and email clients which have been enumerated via software identification, can easily be searched for vulnerabilities using vulnerability text filters within the **Findings** sections of Tenable Vulnerability Management.



Findings

Include Info Severity

All Time

Vulnerabilities

Cloud Misconfigurations

Host Audits

Web Application Findings

< ▾

Advanced

Saved Filters ▾

Search by Assets

Apply

Plugin Name: is equal to "outlook" ×

Clear All

Group By

None

Asset

Plugin

Filters

Apply

Select Filters

Clear All

▼ Plugin Name ▾

is equal to ▾

\*outlook\*

☐ 6 Vulnerabilities

Refresh

Fetch At: 02:59 PM

Grid: Basic View ▾

Columns ▾

1 to 6 of 6 ▾

< >

Page 1 of 1 >

	Asset Name	IPv4 Address	Seve...	Plugin Name	VPR	CVSSv...	State	Sc
<input type="checkbox"/>			High	MS13-068: Vulnerability in Microsoft Outlook Cou...	6.7		Active	Te
<input type="checkbox"/>			Med	MS13-094: Vulnerability in Microsoft Outlook Cou...	2.7		Active	Te
<input type="checkbox"/>			High	MS13-068: Vulnerability in Microsoft Outlook Cou...	6.7		Active	Te
<input type="checkbox"/>			Med	MS13-094: Vulnerability in Microsoft Outlook Cou...	2.7		Active	Te
<input type="checkbox"/>			Med	MS13-094: Vulnerability in Microsoft Outlook Cou...	2.7		Active	Te
<input type="checkbox"/>			High	MS13-068: Vulnerability in Microsoft Outlook Cou...	6.7		Active	Te

Some environments may require or benefit from the use of customized audit files. Organizations have the ability to customize. audit files and tailor audits to their specific needs. For more information on creating custom Tenable Nessus audit files, including examples, review the [Example Audit Items](#) page.

# Learn More

---

## Tenable Resources

- [Email and Web Browser Detections](#)
- [Browser Vulnerabilities Dashboard](#)
- [Cyber Exposure Study: Malware Defenses](#)
- [Compliance Checks Reference Guide](#)

### **NIST Special Publication 800-53 Revision 5**

- CM-10: Software Usage Restrictions
- SC-18: Mobile Code

### **NIST Special Publication 800-53 Revision 4**

- CM-10: Software Usage Restrictions
- SC-18: Mobile Code

### **NIST Special Publication 800-53 Revision 5**

- SC-7: Boundary Protection

### **NIST Special Publication 800-53 Revision 4**

- SC-7: Boundary Protection

### **NIST Special Publication 800-53 Revision 5**

- SI-3: Malicious Code Protection
- SI-8: Spam Protection
- SI-16: Memory Protection

### **NIST Special Publication 800-53 Revision 4**

- SI-3: Malicious Code Protection
- SI-8: Spam Protection
- SI-16: Memory Protection