**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.
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:
The Tenable Security Center Browser Vulnerabilities Dashboard displays actively and passively detected vulnerability information for the major web browsers: Chrome, Firefox, Internet Explorer, Safari, and Opera. An analyst can use this information to determine the browser vulnerabilities, which need to be patched and also if any browsers are being used in unauthorized places.

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.
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:
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.

![Vulnerability Detail List](image)

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.
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**
Chrome Browser Extension Enumeration (98553)

VULNERABILITY

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
https://developers.google.com/chrome/extensions/mac

Output
Incident #: 20000021153

Tenable Security Center
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 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.

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.
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.
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