Tenable Cyber Exposure Study – Email and Web Browser Security

Last Revised: July 17, 2025

Table of Contents

Overview

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."

Email Security

Email is a common attack vector for phishing and malware distribution. Being cautious with links and attachments, especially from unknown senders, and utilizing email services with phishing protection and spam filtering are key strategies. Additionally, encryption protocols, such as Transport Layer Security (TLS) to encrypt email in transit, and End-to-End encryption can add additional layers of protection to secure email.

Email authentication protocols, such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC), Multifactor Authentication (MFA), combined with regular patching and updates provide methods to prevent messages from being tampered with, protect against spoofing, add additional layers of security, and reduce a bad actor's ability to utilize weakness to exfiltrate information.

Web Browser Security

Browsers are the gateway to the internet, and just like email they are frequent targets for malware and scams. To stay vigilant, utilize Secure Connections (HTTPS), keep browsers up to date, and disable unnecessary plugins.

AI/LLM and Web Browsers

Artificial Intelligence (AI) and Large Language Models (LLM) offer useful functionality, and can pose some security risks simultaneously. The risk is inherent on how the plugin is designed, how the plugin handles data, and what permissions are required for the plugin to function properly. Some key security concerns are:

- **Data Privacy and Leakage** - AI plugins require text input and connection to an outside server. This can potentially lead to confidential information being leaked.
- **Unauthorized Access** - Plugins with extensive permissions have the potential to be exploited, allowing attackers to monitor activity.
- **Malicious Code Injection** - A compromised plugin could potentially inject malicious code leading to Cross-Site Scripting (XSS), or man-in-the-middle attacks.
- **Dependency on Third-Party Applications** - Many AI plugins rely on third-party APIs. If the API is compromised attackers could gain access to sensitive data.
- **Security Vulnerabilities in AI Models** - A new attack that is becoming more commonplace with AI/LLM is a Prompt Injection Attack. A prompt injection attack occurs when an attacker manipulates the AI model into influencing the output, thereby leading to the possible disclosure of sensitive information. Prompt injection attacks were named by OWASP as a top security threat to LLMs.

How Tenable Can Help

Clicking on malware designed to deceive users, either inside of an email or on a malicious website, is a very common and successful method of attack. This method is best cured with a solid cybersecurity awareness program. Awareness 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.

Knowing what email and web browser applications are installed, as well as their plugins is critical to protecting your organizations. 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.

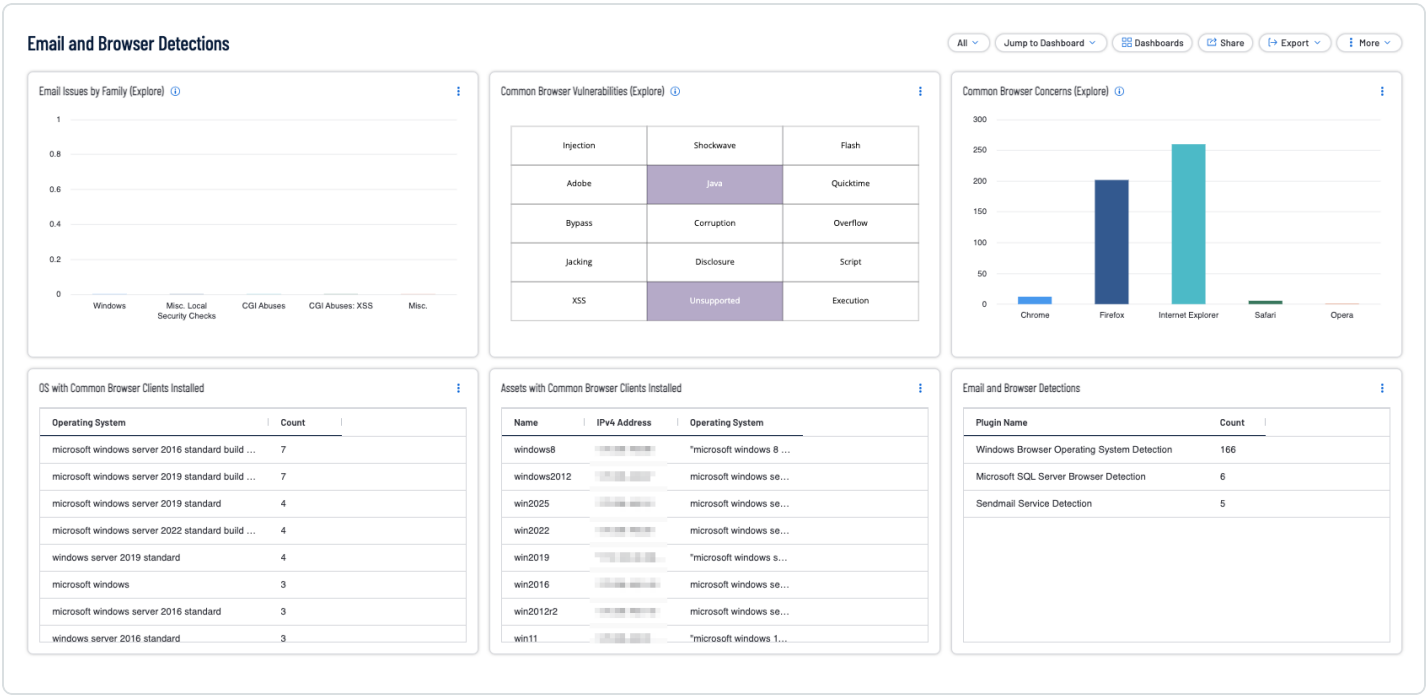
To mitigate these vulnerabilities, users and organizations should practice safe email and web browsing habits, keep software up-to-date, and utilize anti-virus and anti-phishing software, and only install approved applications and plugins. Tenable can assist organizations to reduce these threats by minimizing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

Tenable leverages a variety of products within our portfolio to effectively manage and prioritize business exposure across the entire attack surface. Exposure management is a set of processes and technologies that assess the accessibility, exploitability, and criticality of digital assets across the modern attack surface. Exposure Management is the natural evolution of existing vulnerability management programs, elevating factors like likelihood of attack, human and machine permissions, viability of attack paths, and potential business impact. Cyber Exposure Studies help organizations build a path which focuses on the products and methods that best assist organizations with a specific goal in mind.

Ensure the Use of Only Fully Supported Email and Browser Clients

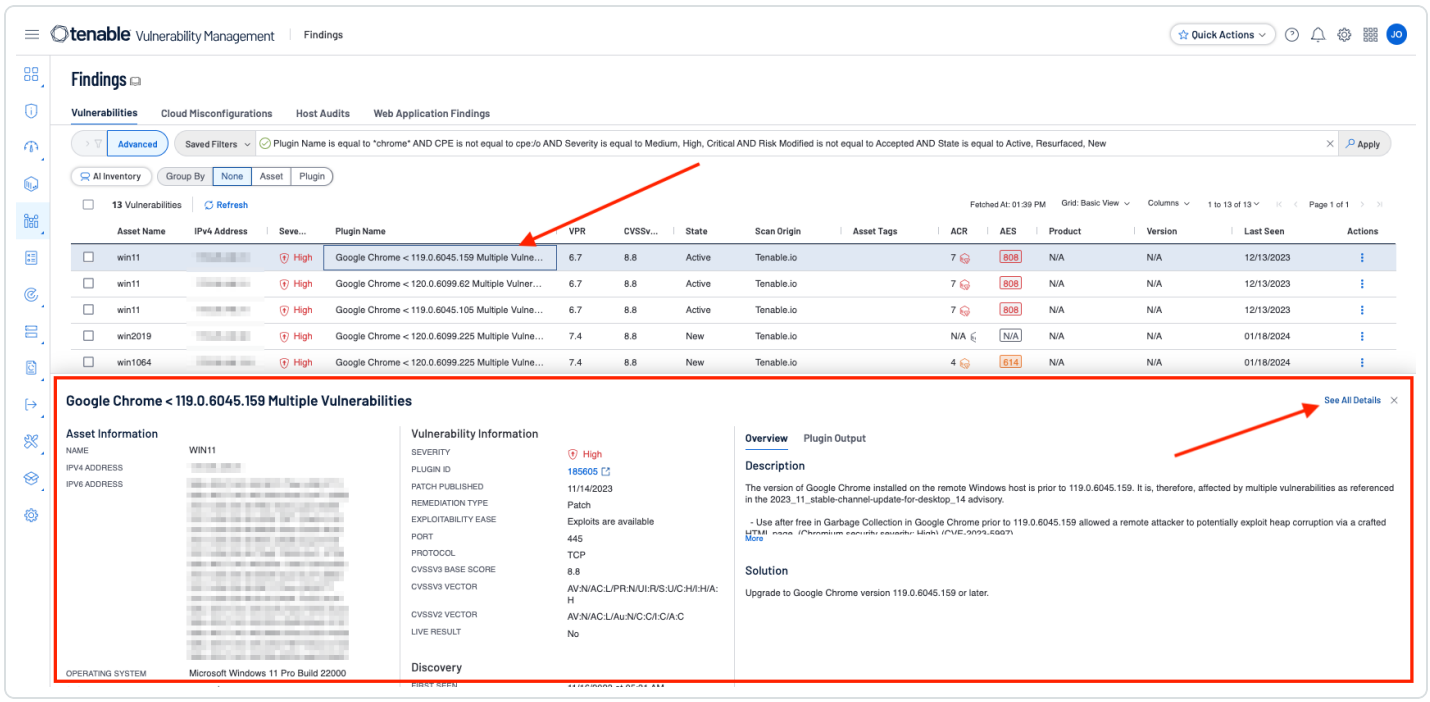
Tenable products allow security operation teams to use Tenable One to analyze endpoint browser and email client configurations. Using a variety of active and passive plugins paired with Tenable Vulnerability Management, the organization can verify that established configuration policies are

followed. Tenable provides several solutions for organizations to better understand vulnerability management. As an example, the Tenable 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:

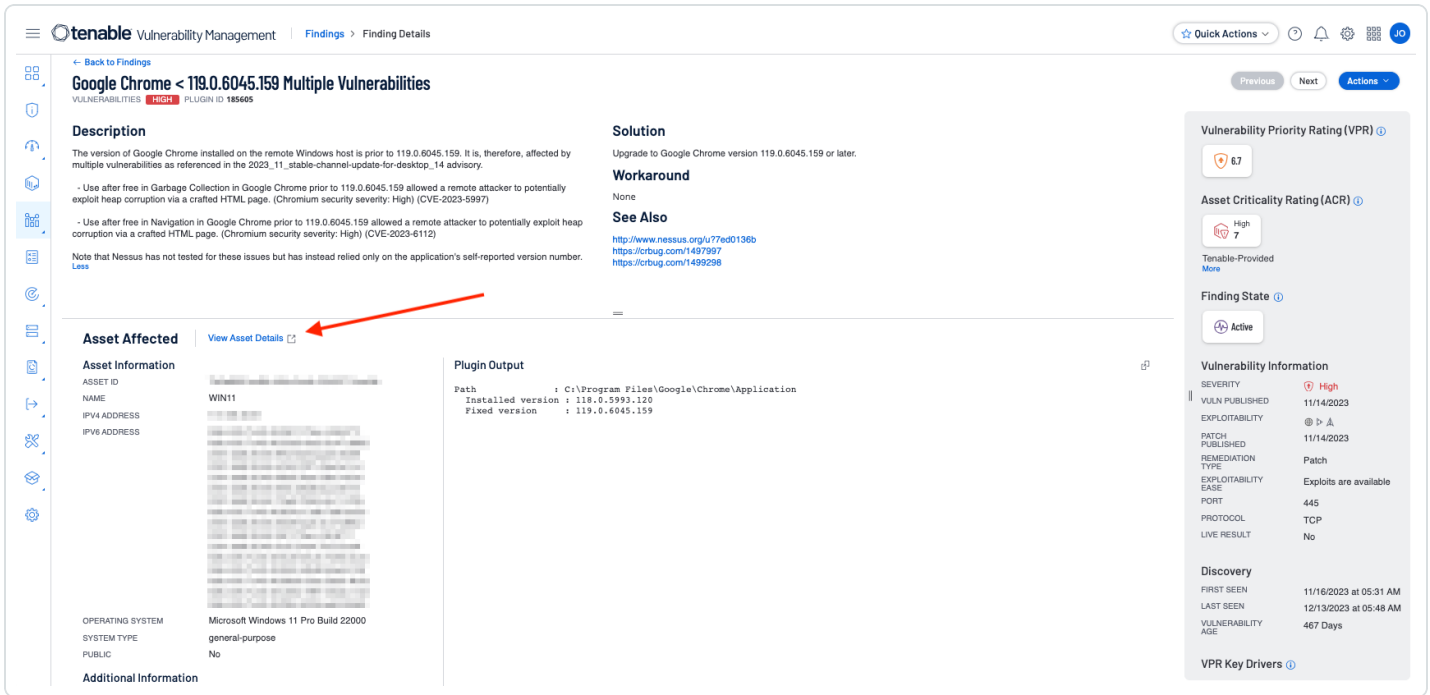


Drilling Down in Tenable Vulnerability Management

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.



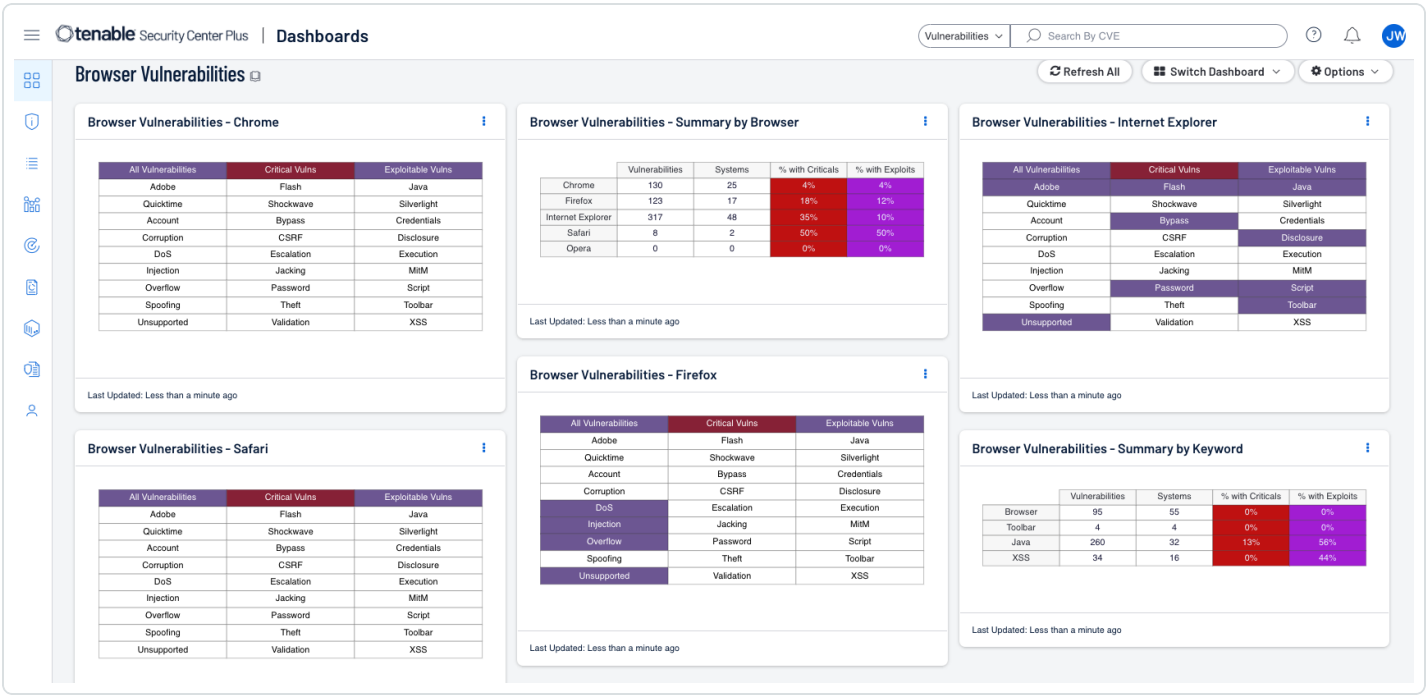
Clicking on **See All Details** opens the **Details** page. The details page provides a wealth of information, including the description, solution, asset details, and key findings on the right side of the page, as shown in the following image:



Note: The Details page contains a link to View Asset Details. Clicking this link will present a page highlighting all the known vulnerabilities that have been associated with this particular asset.

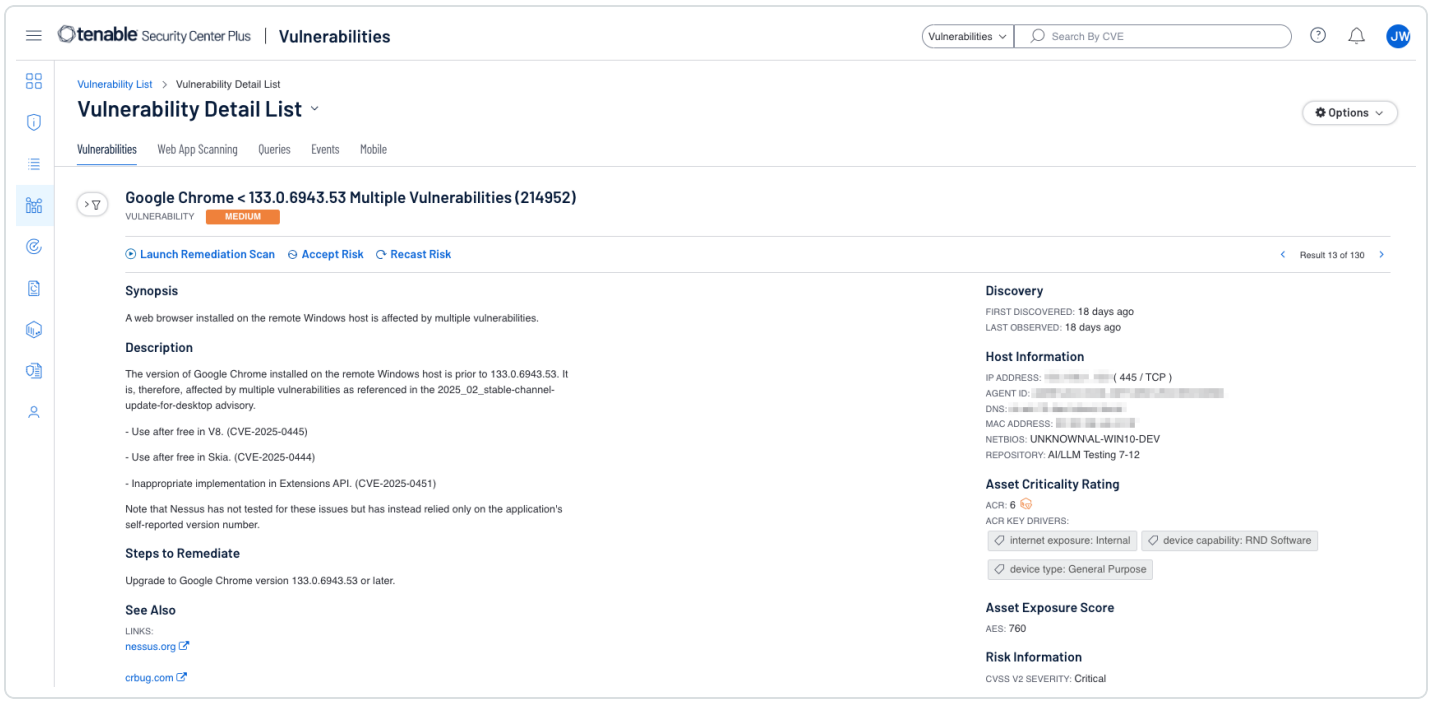
The Tenable Security Center Browser Vulnerabilities Dashboard displays actively and passively detected vulnerability information for the major web browsers: Chrome, Firefox, Internet Explorer, Safari, and Opera. An analyst can use this information to determine the browser vulnerabilities, which need 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.

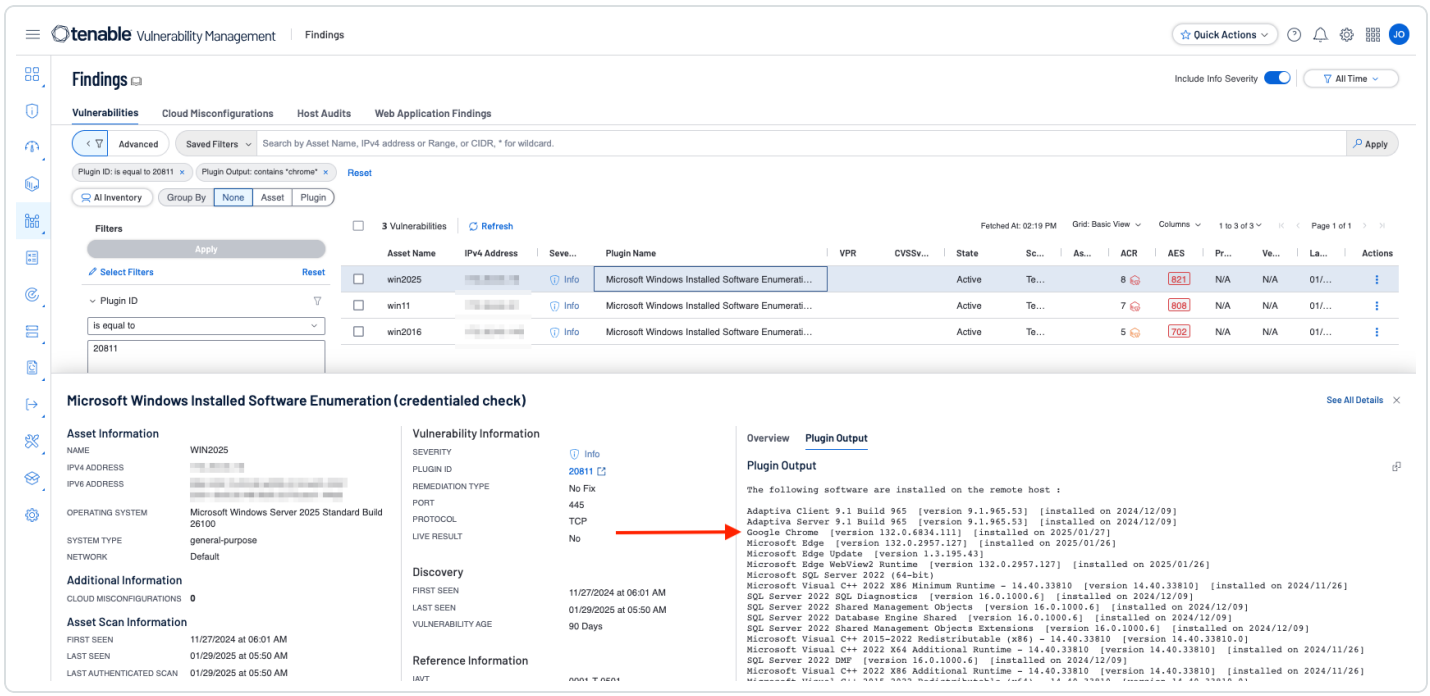


As discussed, reducing the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems is a critical effort. One of the most important aspects of this effort is the identification of installed web and email applications. 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 Applications

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 in Tenable Vulnerability Management, or the Analysis Page within Tenable Security Center, and apply the above filter, then view the details and the plugin output. Results similar to the following screenshot will be displayed.



Note: For Tenable Security Center, the process has the following differences. From the Analysis tab, filter on pluginID = 20811, with a Vulnerability Text contains chrome (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 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

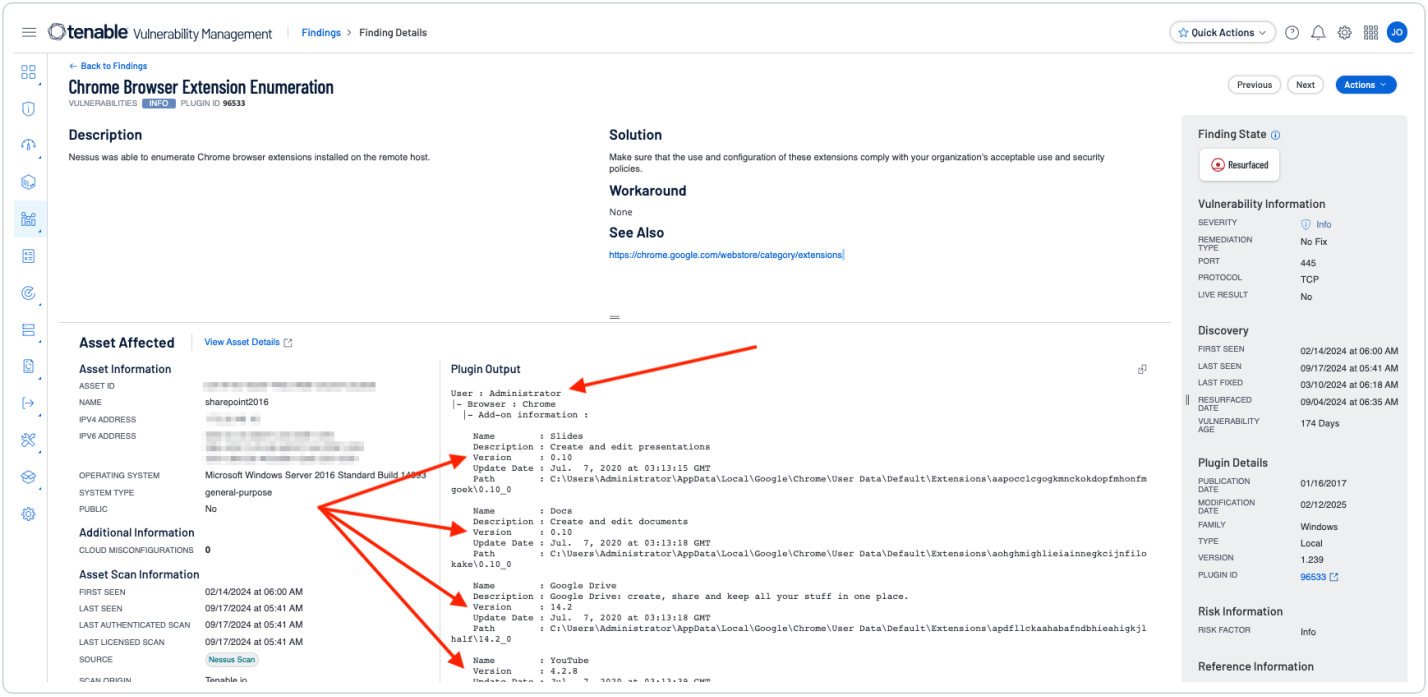
Organizations need to determine which browser extensions are authorized, and which ones are not. Once this determination is made, restrict either through uninstalling or disabling any unauthorized or unnecessary browser or email client plugins, extensions, and add-on applications.

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 the example below (Tenable Vulnerability Management shown), 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.

AI/LLM Detection

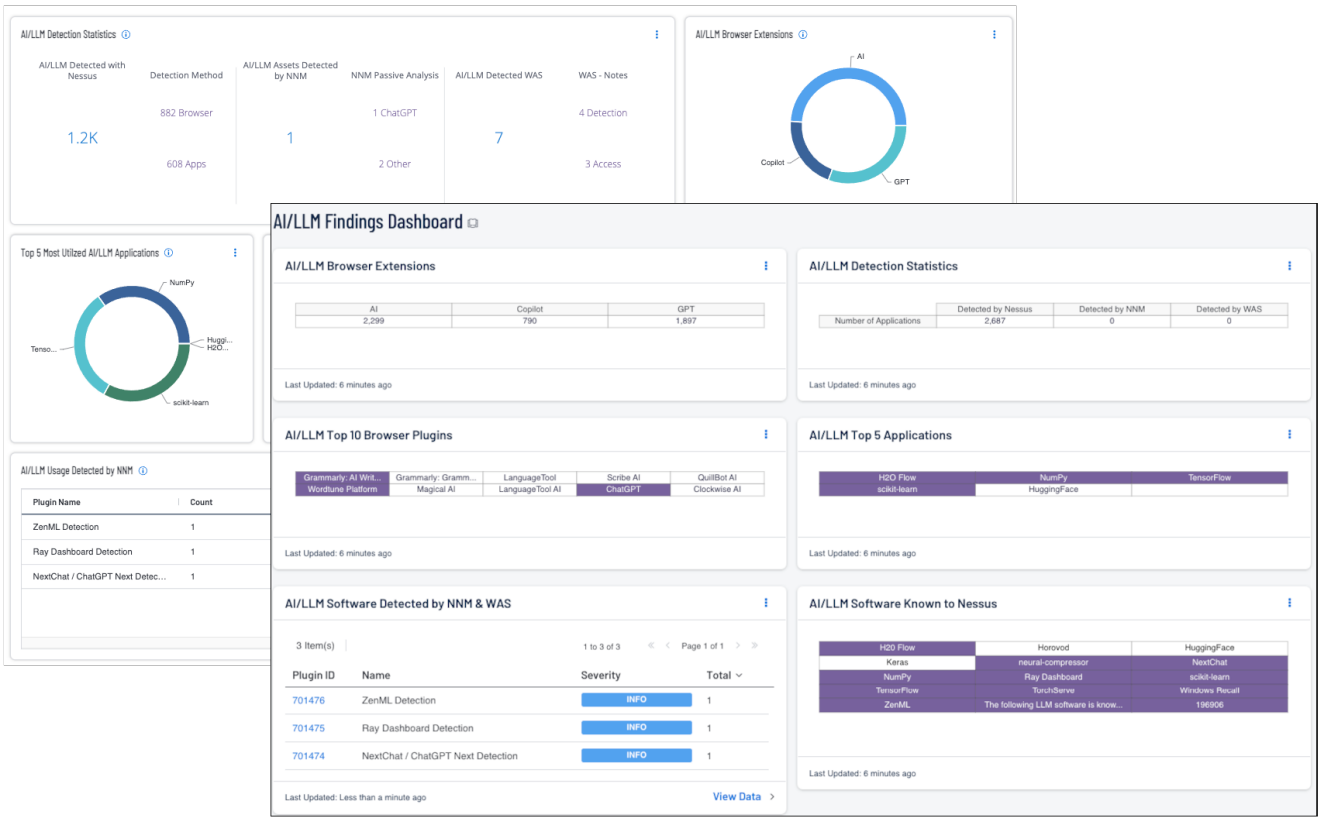
In an era of rapidly evolving Artificial Intelligence/Large Language Model (AI/LLM) technologies, cybersecurity practitioners face significant challenges in monitoring unauthorized AI solutions,

detecting AI vulnerabilities, and identifying unexpected AI/LLM development. Tenable leverages advanced detection technologies - agents, passive network monitoring, dynamic application security testing, and distributed scan engines - to surface AI/LLM software, libraries, and browser plugins. The risk managers utilize this data to begin a comprehensive review of the AI/LLM packages in systems and web applications, along with associated vulnerabilities, mitigating risks of exploitation, data leakage, and unauthorized resource consumption.

The Nessus AI/LLM Software Report plugin (196906) reports a summary of all AI/LLM software detected on the remote host. This plugin detects AI/LLM usage in 3 ways: browser extensions, applications, and file paths all common to AI/LLM implementations. AI/LLM vulnerabilities discovered in web applications are identified using the Web Application Scanner, alongside network traffic analysis using the Nessus Network Monitor (NNM). By combining all methods of data collection, the risk managers are able to identify problem areas and other risks associated with AI/LLM.

AI/LLM technologies are promising and can transform many industries and businesses, offering new innovation and efficiency opportunities. However, the technology represents a huge security challenge at many layers and this impact should not be overlooked. By using Tenable Security Center and Tenable Web App Scanning the organization is able to take a security-first approach. When combined with best practices and robust governance policies, the organizations can harness the power of AI/LLM and mitigate the associated emerging threats.

The AI/LLM Findings dashboard for Tenable Security Center and Tenable Vulnerability Management (both displayed below) provides detailed information on AI/LLM findings in web browser extensions and applications.



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

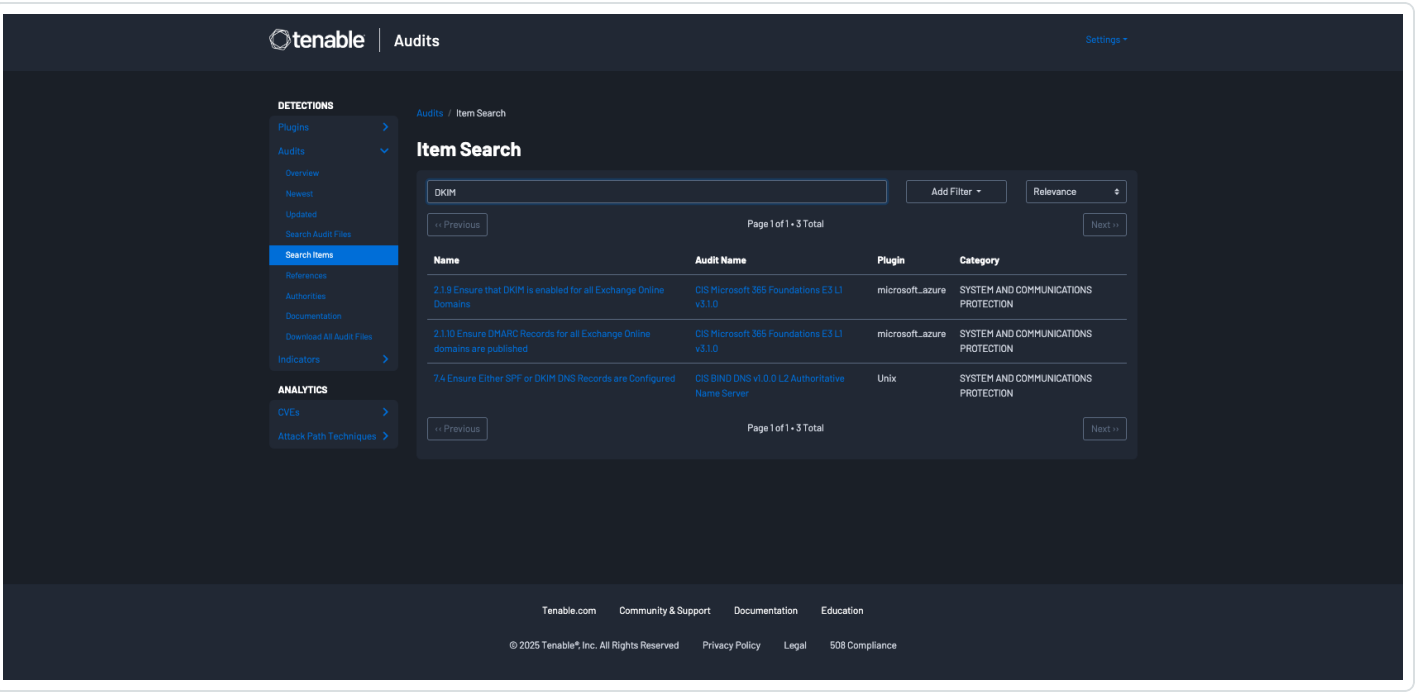
SPF, DKIM, and DMARC

Sender Policy Framework (SPF) is an email authentication method which helps prevent email spoofing by checking the SPF record that is published in the domain owner's Domain Name System (DNS). SPF results are utilized by DMARC.

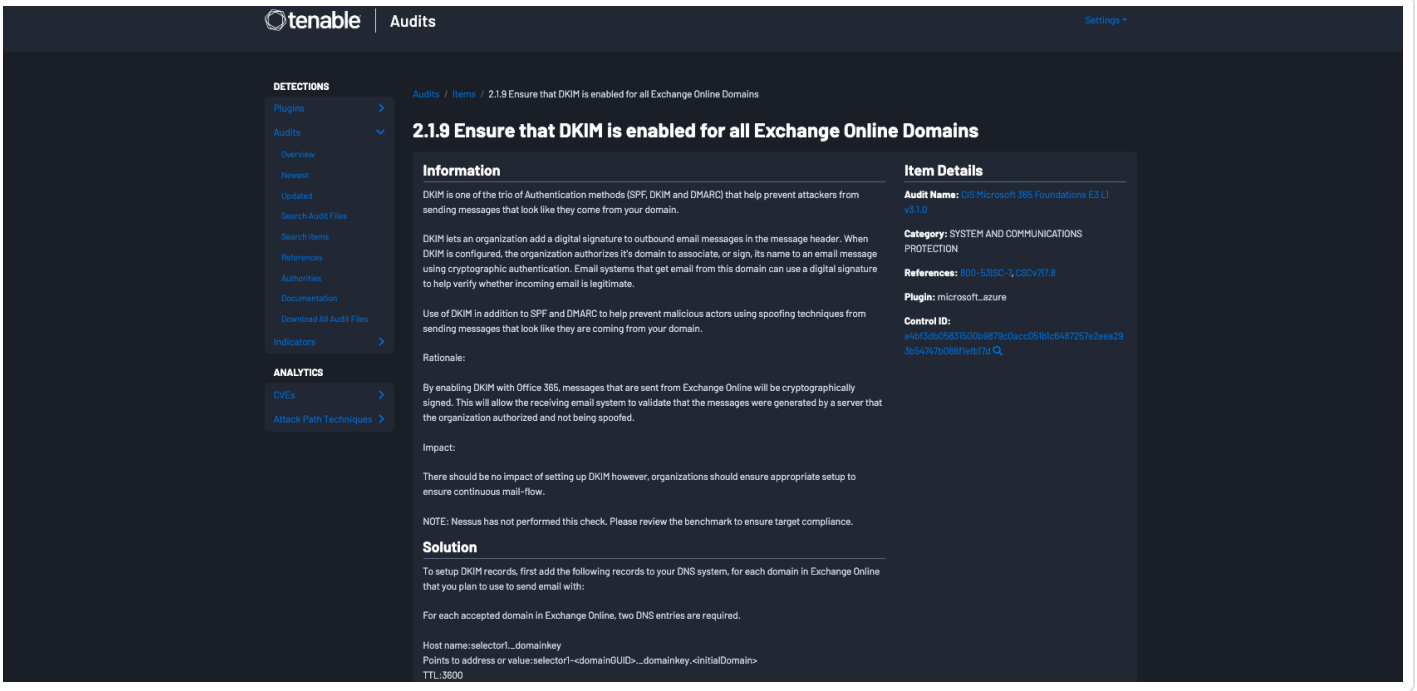
DomainKeys Identified Mail (DKIM) is an authentication method which detects forged sender addresses in email. Forging signatures is a technique used in many phishing and email spam campaigns. DKIM allows the recipient to check the email signature and ensure the email came from the domain stated.

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.

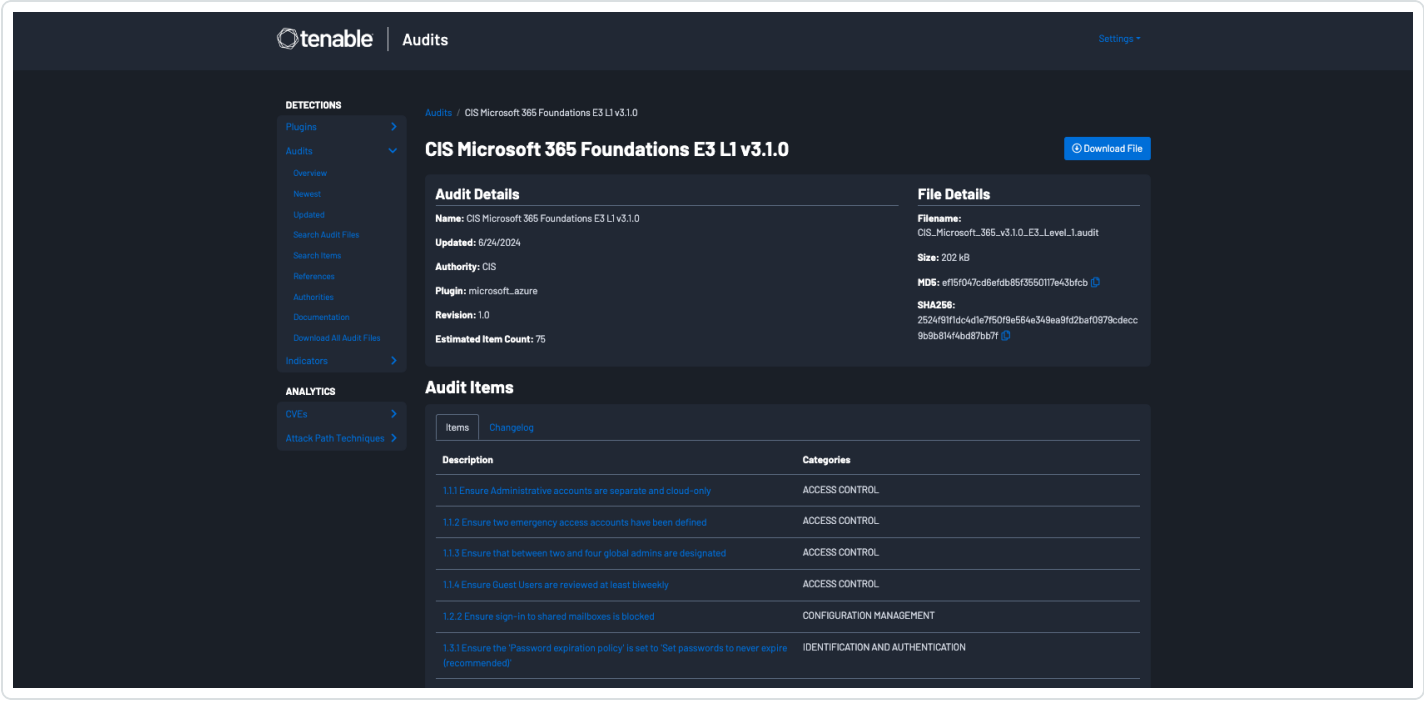
Tenable has audit files for Microsoft (CIS Microsoft 365 Foundations E3 L1 v1.5.0) that check for SPF, DKIM, and DMARC records. Additionally, an audit file (CIS BIND DNS v1.0.0 L2 Authoritative Name Server) for Unix systems, containing checks to ensure Either SPF or DKIM DNS Records are configured, is 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, 2.1.9 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 v3.1.0, provides a description of the audit items, and a download button in the top right corner.

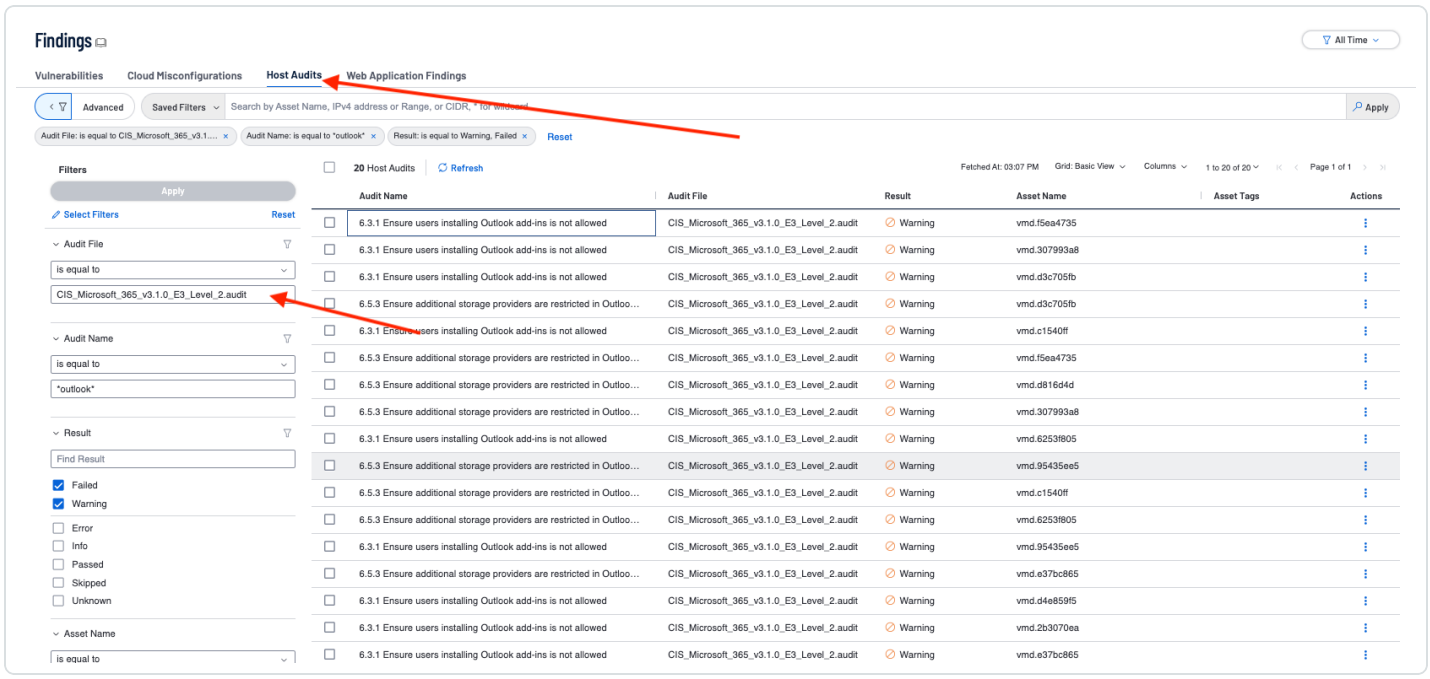


For information related to adding an audit file to Tenable Security Center, refer to the Audit File section of the Tenable documentation site.

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. The following results are available from the **Host Audit** section within the **Findings** page using filters for the audit file specified above, and filtering down to only include Outlook and either Failed or Warning audit results..



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