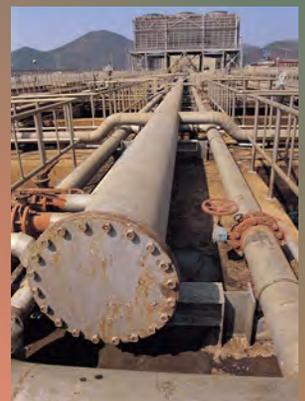


U.S. International Trade Commission

Audit of the USITC's Patching of Critical and High Vulnerabilities on the International Trade Commission Network



OIG-AR-22-10

September 19, 2022



Office of Inspector General

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency that provides trade expertise to both the legislative and executive branches of government, determines the impact of imports on U.S. industries, and directs actions against certain unfair trade practices, such as patent, trademark, and copyright infringement. USITC analysts and economists investigate and publish reports on U.S. industries and the global trends that affect them. The agency also maintains and publishes the Harmonized Tariff Schedule of the United States.



UNITED STATES INTERNATIONAL TRADE COMMISSION
OFFICE OF INSPECTOR GENERAL
WASHINGTON, DC 20436

IG-UU-009

September 19, 2022

MEMORANDUM

TO: David S. Johanson, Chairman

FROM: Rashmi Bartlett, Inspector General *Rashmi Bartlett*

SUBJECT: Audit of USITC's Patching of Critical and High Vulnerabilities on the International Trade Commission Network Final Report

This memorandum transmits the final report for the Audit of the USITC's Patching of Critical and High Vulnerabilities on the International Trade Commission Network, OIG-AR-22-10. In finalizing this report, we analyzed management's comments on our draft report and have included those comments in their entirety as Appendix A.

The objective of the audit was to determine whether the Commission was patching critical and high vulnerabilities effectively on ITCNet. The audit determined that components of the Commission's vulnerability management program were not effective in patching critical and high vulnerabilities on the ITCNet.

The report contains three recommendations. In the next 30 days, please provide me with your management decisions describing the specific actions that you will take to implement each recommendation.

We will post this report on our website at www.usitc.gov/oig.

U.S. International Trade Commission

Audit Report

***Audit of the USITC’s Patching of Critical and High Vulnerabilities on
the International Trade Commission Network***

Table of Contents

***Background* 1**

 Purpose.....1

 Introduction.....1

***Results of Audit* 6**

 Problem Area 1: Scanning Core Infrastructure Systems 8

 Problem Area 2: Managing Critical and High Vulnerabilities Older than 30 Days 12

***Management Comments and OIG Assessment* 15**

***Objective, Scope and Methodology*..... 15**

***Appendix A: Management Comments*..... 17**

***Appendix B: Common Vulnerability Scoring System (CVSS)*..... 18**

U.S. International Trade Commission

Audit Report

Chapter 1

Background

Purpose

The U.S. International Trade Commission's (Commission) Office of Inspector General conducted this audit to determine if the Commission effectively patches critical and high vulnerabilities on the International Trade Commission Network, known as ITCNet. The ITCNet includes the hardware, software, applications, databases, communications, and Internet access to support the Commission's mission and daily operations.

Introduction

A vulnerability is a software flaw or weakness that, if exploited to obtain unauthorized access, could negatively impact information technology systems and data. Vulnerabilities are classified as critical, high, medium, or low in the order of severity. According to the National Institute of Standards and Technology (NIST) figures, the total number of vulnerabilities reported has steadily increased over the last five years.¹ The threat of vulnerabilities requires information technology managers to continuously manage and monitor, patch, scan, and prioritize systems for mitigation. Managers involved in vulnerability patching also consider the level of risk when deciding whether and when to accept vulnerabilities that cannot be patched during the established patching timeframe.

The federal government and the Commission have defined thresholds for identifying and remediating vulnerabilities,² listed from greatest to least risk below.

Federal Government Thresholds

- a) **Cybersecurity and Infrastructure Security Agency (CISA)³ Known Exploited Vulnerabilities** – Remediate each vulnerability according to the timelines outlined in the

¹ NIST CVSS Severity Distribution Over Time <https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time>.

² Remediating refers to fixing or patching a vulnerability.

³ The Cybersecurity and Infrastructure Security Agency (CISA), within the Department of Homeland Security. See www.cisa.gov for additional details.

U.S. International Trade Commission

Audit Report

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA)'s [Binding Operational Directive 22-01](#).

- b) **Servers Accessible from the Internet** – Remediate critical vulnerabilities within 15 days and high vulnerabilities within 30 days from initial detection per CISA's [Binding Operational Directive 19-02](#).

Commission Thresholds

- a) **Non-Internet Accessible Systems** – Critical and high vulnerabilities are to be remediated within 30 days from being first discovered, according to the Commission's internal patching process.

The Commission uses the Common Vulnerability Scoring System (CVSS) to determine which vulnerabilities are critical or high. CVSS is a vulnerability scoring system designed to provide a standardized method for rating information technology vulnerabilities. It is used to calculate the severity of vulnerabilities found on a system and as a factor in prioritizing vulnerability remediation activities. The U.S. government's National Vulnerability Database, a repository of vulnerability management data, has CVSS scores for almost all known vulnerabilities. Additional details on the CVSS can be found in Appendix B.

Vulnerability Management

Vulnerabilities more than 30 days old must be actively managed, tracked, and reported timely to OCIO leadership so that security risks can be understood and addressed. In our review of guidance from NIST and the SANS Institute, the world's largest cybersecurity and research organization, we identified components of an effective vulnerability management program:

1. Actively managing authorized assets.
2. Reviewing and prioritizing vulnerabilities.
3. Continuously patching software vulnerabilities.
4. Routinely scanning to detect and report on system vulnerabilities.
5. Manage risk through reporting and communicating vulnerabilities.

U.S. International Trade Commission

Audit Report

Actively Managing Authorized Assets

Actively managing authorized assets is a core foundational security control, a process that identifies the assets that need to be continuously monitored, scanned, and remediated for vulnerabilities. The OCIO maintains its authorized assets in a computer system database that the Cybersecurity Services Division manages.

Reviewing and Prioritizing Vulnerabilities

The OCIO continuously reviews and prioritizes vulnerabilities. The Cybersecurity Services Division generates multiple scanning reports to identify and manage vulnerabilities. The division is responsible for alerting OCIO leadership when vulnerabilities are older than 30 days from the first discovered date. OCIO generates weekly reports that list new and previously identified system vulnerabilities which have not been addressed. Once a vulnerability has been remediated, it no longer appears on the report. The report also contains metrics on patches that have been applied (since the last report) to fix vulnerabilities. The metrics allow OCIO to determine whether patching is occurring within expected (or required) timeframes.

According to the Commission's Information System Security Officer:

Identified flaws in ITCNet are addressed and reported to the Network Services Division (Servers) and the Service Delivery Division (Workstations). The Commission's workstations are patched 30 days for CVSS high and critical vulnerabilities and 90 days for moderate and below. Server updates and patches are tested by Engineering in the testing environment before installation in the production environment. When zero-day vulnerabilities⁴ and/or federal mandates require a patch deployment schedule that is more aggressive than the timelines stated above, the CSD will notify the Network Services Division (Servers) and the Service Delivery Division (Workstation) of the special timelines.

Continuously Patching Software Vulnerabilities

OCIO is responsible for identifying and continuously patching vulnerabilities on the USITC's network. Each of OCIO's four divisions plays a part in patching vulnerabilities on the network:

⁴ [A zero-day vulnerability](#) exploits a previously unknown hardware, firmware, or software vulnerability. Because zero-day vulnerabilities are discovered before security researchers and software developers are aware of them and can issue a patch, they pose a high risk.

U.S. International Trade Commission

Audit Report

1. **Service Delivery Division** patches all workstations and laptops (Windows 10 systems) on the network using Microsoft's System Center Configuration Manager (SCCM⁵).
2. **Network Services Division** patches
 - a. Windows servers with SCCM
 - b. Linux Systems with Red Hat Satellite⁶
 - c. Network devices with Cisco Prime⁷
3. **Software Engineering Division** patches all software related to software development.
4. **Cybersecurity Division** patches cyber security tools and oversees the vulnerability management program.

Routinely Scanning to Detect and Report on System Vulnerabilities

The Commission uses the scanning tool Tenable.sc software daily to detect, evaluate, and report vulnerabilities on ITCNet. According to the Tenable company, Tenable.sc is used by more than 40,000 organizations worldwide, including many federal agencies, to understand and reduce the risk of vulnerabilities.⁸ The U.S. Department of Homeland Security includes Tenable.sc in its Continuous Diagnostics and Mitigation (CDM) program.⁹

OCIO uses Tenable.sc to scan systems, workstations, and servers across the Commission's network, ITCNet. The tool gathers and evaluates vulnerability data, identifies trends, and prioritizes vulnerabilities based on its calculation of risk. Tenable.sc uses the CVSS scoring system to classify the critical and high vulnerabilities found on ITCNet.

⁵ SCCM is a tool that tracks and applies software updates to Windows workstations and servers.

⁶ Red Hat Satellite patches Red Hat Linux servers.

⁷ Cisco Prime is a device operation, administration, and network management solution.

⁸ See <https://www.tenable.com/about-tenable/about-us> and <https://investors.tenable.com/>.

⁹ The CDM Program was developed in 2012 to support government-wide and agency-specific efforts to provide risk-based, consistent, and cost-effective cybersecurity solutions to protect federal civilian networks across all organizational tiers.

U.S. International Trade Commission

Audit Report

Manage Risk Through Reporting and Communicating Vulnerabilities

OCIO has defined the process for managing risk and reporting on vulnerabilities older than 30 days in a standard operating procedure (SOP) called, *Vulnerabilities Older than 30 Report Procedures*. The three steps of the process are:

1. The Commission's Cybersecurity Services Division creates the "Vulnerabilities Older than 30" report.
2. The other three IT divisions (Service Delivery, Network Services, and Software Engineering) add to the report the reason their systems have vulnerabilities older than 30 days, why the vulnerabilities are not patched, and how the vulnerabilities will be remediated.
3. The Information Systems Security Officer (ISSO) provides a vulnerability status report that includes the items above to the Chief Information Officer (CIO) each month.

U.S. International Trade Commission

Audit Report

Chapter 2

Results of Audit

We found that components of the Commission’s vulnerability management program were not effective in patching critical and high vulnerabilities on the ITCNet. The Commission reviews and prioritizes vulnerabilities on the ITC network, continuously patches with its systems management tools, and routinely scans and reports on vulnerabilities. However, during the period we reviewed from January 2022 to March 2022, we identified gaps in the Commission’s process for identifying and tracking critical and high vulnerabilities. As a result, critical and high vulnerabilities were not effectively tracked. For example, USITC scanned systems that were not on the network-approved list, and other systems were neither scanned nor on the authoritative list. Moreover, the Commission had challenges tracking vulnerabilities over 30 days due to fluctuations in the first discovery date calculated by its scanning software.

The Commission made changes during our audit to address gaps in the management of critical and high vulnerabilities. In addition, we identified two areas where further improvements can enhance the Commission’s controls over the patching and management of critical and high vulnerabilities: the scanning of infrastructure systems and the tracking of the first discovery date.

The USITC’s core infrastructure system is dynamic, and new devices and software are constantly being added or removed. Therefore, it is important for the Commission to effectively manage all systems to reduce security risks. Table 1 summarizes the results for each vulnerability program component we reviewed and identifies whether the Commission fully met, partially met, or did not meet the criteria for an effective program. The criteria for effectiveness includes that 95% of hardware assets are monitored, which OCIO reported to the Office of Management Budget in FY 2021.

U.S. International Trade Commission

Audit Report

Table 1: Vulnerability Program Components Across ITCNet

VULNERABILITY PROGRAM COMPONENT	SYSTEM TYPE			
	Windows 10 Laptops & Workstations	Windows Servers	Linux Servers	Network Devices
Actively Managing Authorized Assets	◐	◐	◐	◐
Review and Prioritize Vulnerabilities	●	●	●	●
Continuously Patching Vulnerabilities	●	●	●	●
Routinely Scan & Report Vulnerabilities	●	●	●	●
Manage and Track Vulnerabilities	◐	◐	◐	◐
Legend:	● Fully Met ◐ Partially Met ○ Not Met			

Source: U.S. International Trade Commission Office of Inspector General assessment, based on NIST SP 800-40r4 Guide to Enterprise Patch Management Planning¹⁰ and SANS Vulnerability Management Maturing Model¹¹

As demonstrated in Table 1, the Commission met its criteria for reviewing, prioritizing, and patching vulnerabilities. However, the Commission only partially met its criteria for actively managing authorized assets and tracking vulnerabilities. Because of these gaps in the vulnerability management program, the Commission cannot be assured that systems on ITCNet have been scanned and known critical and high vulnerabilities patched. System vulnerabilities should be patched to prevent attackers from obtaining unauthorized access to a system or device, which could be used as a platform to compromise the Commission’s network.

We analyzed the cause of the gaps in the Commission’s process and the Commission’s ability to meet the criteria in Table 1 and identified two main problem areas for improvement:

- (1) Scanning core infrastructure systems and
- (2) Managing critical and high vulnerabilities older than 30 days.

¹⁰ NIST SP 800-40r4, [Guide to Enterprise Patch Management Planning](#)

¹¹ SANS [Vulnerability Management Maturity Model](#)

U.S. International Trade Commission

Audit Report

Problem Area 1:

Scanning Core Infrastructure Systems

One of the critical components of an effective vulnerability management program is to scan continuously the network for vulnerabilities. The Commission’s authoritative list shows what’s approved and authorized to be on the network. The Tenable.sc vulnerability tool can generate its own systems list to scan authorized systems for vulnerabilities. OCIO’s responsibilities include identifying, analyzing, and addressing discrepancies between authorized and unauthorized systems on the ITCNet to protect the Commission from the risk of vulnerabilities on unapproved and unmanaged assets.

USITC shall scan for vulnerabilities in the information system and hosted applications daily and when new vulnerabilities potentially affecting the system/applications are identified and reported.

Source: ITCNet’s System Security Plan, dated January 31, 2022

Table 2 represents our analysis to determine whether the Commission was scanning authorized systems for vulnerabilities. We asked OCIO to provide us with a list of devices authorized to be on the network. During January and March 2022, we found that, of the total number of systems on the Commission’s authorized list, over a third (36%) were not scanned by Tenable. Most of the systems on the authorized list not scanned were Network and Windows 10 systems.

Tenable did not scan all authorized devices because the authoritative list was not up to date. When we met with the CIO to discuss our preliminary report, we were told that OCIO uses data from multiple tools – SCCM, Red Hat Satellite, and Cisco Prime – to determine what systems need to be patched. However, the OCIO acknowledged that the office has not been reconciling what is patched against what should be patched.

Table 2. Authorized Systems Not Scanned by Tenable

System Type	Authorized	
	Total	Not Scanned by Tenable
Windows 10	421	191
Windows Servers	57	13
Network	78	46
Linux Servers	165	10
Total	721	260

Source: OIG review of OCIO authoritative list and Tenable.sc list of scanned systems

U.S. International Trade Commission

Audit Report

As shown in Table 3, the Tenable software program scanned systems on the ITC Network that were not on the Commission’s authorized list, including 148 Windows 10 systems, 47 Windows servers, 65 Network devices, and 147 Linux servers. In total, Tenable found and scanned an additional 407 systems that were not on the Commission’s authorized list. The difference in the number of systems scanned resulted from the authoritative list not being up to date.

Table 3. Unauthorized and Authorized Systems Scanned by Tenable

System Type	Unauthorized Systems on the Commission Network	Authorized Systems on the Commission Network and Scanned by Tenable	Number of Systems on the Commission Network Scanned by Tenable
Windows 10	148	230	378
Windows Servers	48	44	92
Network	65	32	97
Linux Servers	147	155	302
Total	407	461	868

Source: OIG review of OCIO authoritative list and Tenable.sc list of scanned systems

We found that the Commission did not have adequate controls to maintain a comprehensive, accurate inventory of authorized hardware. We identified problems with updating the authorized hardware list in a 2019 audit report¹² and recommended that the USITC develop a process to ensure the authoritative hardware database is kept up to date. In response to our recommendation, the Commission told us that it completed corrective action and developed and implemented a backup process for detecting and preventing unauthorized devices on ITCNet.

For the patching of critical and high vulnerabilities, there was also no process in place to verify that all authorized systems were scanned for vulnerabilities. This problem is consistent with the findings identified in our 2021 audit of ITCNet’s security log management system,¹³ during which we found that the Commission did not effectively collect, analyze, or review security logs from all systems. In this case, as with the 2021 audit, the use of software alone to manage vulnerabilities – without monitoring controls and reconciliation of disparate inventories – is not sufficient to ensure all authorized devices are scanned for vulnerabilities and unauthorized devices are flagged, given the highly dynamic nature of assets. According to NIST, “A realistic goal is to maintain a close-to-comprehensive inventory by relying on automation to constantly

¹² Audit of ITCNet’s Hardware Management [OIG-AR-20-07](#).

¹³ Audit of ITCNet’s Security Log Management System [OIG-AR-21-08](#).

U.S. International Trade Commission

Audit Report

discover new assets and collect up-to-date information on all assets.”¹⁴ NIST guidance explains that there are two ways for an organization to manage its authorized assets with a high level of accuracy and maintain updated records:

1. Using a Configuration Management Database (CMDB), which would store information about hardware or software in the IT environment¹⁵
2. Splitting responsibility for the authoritative list among multiple resources instead of a single list

Of the Commission’s systems, Windows 10 laptops and workstations had the highest number of unscanned assets due to the challenges of scanning laptops over the USITC’s virtual private network (VPN). In addition to the gaps in the scanning of Windows 10 systems, we discovered a significant difference between the number of Windows 10 systems reported by the Commission to the Department of Homeland Security for the quarter ending March 2022¹⁶ and what was reported as scanned that month. The Commission reported 547 Windows 10 workstations. As shown in Table 3, only 230 of those systems were authorized and scanned. This is significant as over half of the Windows 10 systems on the ITCNet were unauthorized and not scanned.

The OCIO identified a problem scanning Windows 10 systems due to connectivity to the VPN and addressed it by sending users periodic email reminders to connect to the VPN for four hours or longer. A shorter connectivity time that does not allow sufficient time for scanning can occur when:

- Users access email and collaboration and communication software such as Microsoft Teams and either do not stay connected to the VPN or may not connect to the VPN.
- Users are only on the VPN briefly to access resources on the USITC’s intranet or complete biweekly timesheets.

When there is insufficient time for scans to complete, the Cybersecurity Services Division lacks insight into the vulnerabilities on the network. For example, there may be both critical and high vulnerabilities that cannot be fully scanned due to a lack of time on the VPN. In addition, because of not thoroughly scanning the core infrastructure, the Commission may have

¹⁴ NIST Guide to Enterprise Patch Management Planning SP 800-40r4, Chapter 3 Recommendations for Enterprise Patch Management-3.2 Inventory your Software and Assets.

¹⁵ CMDB stores information about hardware and software assets in your IT environment.

¹⁶ OCIO reports metrics each quarter to the Department of Homeland Security as required by the Federal Information Security Management Act (FISMA).

U.S. International Trade Commission

Audit Report

vulnerabilities that could expose sensitive data and compromise data integrity and availability of the Commission's network for users.

During our review, the OCIO deployed Cisco's AnyConnect Client Management VPN Tunnel to all USITC users. This change will allow OCIO to continuously patch and scan Windows 10 systems, even when users are not connected on the VPN. The Commission implemented this change in May 2022. We agree that this is a necessary and important step to address the gaps in scanning laptops. In order to identify and address anomalies going forward, USITC will need to verify scanning performed by automated tools against what should be on the network.

Recommendation 1: Complete the necessary steps to implement a technical control to confirm that core infrastructure systems on the network are being scanned to detect critical and high vulnerabilities.

Recommendation 2: Develop a process to: 1) verify that all authorized devices are being scanned or prioritized for scanning, 2) remove unauthorized devices from the network, 3) implement a tool or a process to monitor whether all authorized devices are being scanned, and 4) reconcile the authoritative list of systems approved to be on the network against the list of scanned devices at regular intervals for differences and keep the list up to date.

U.S. International Trade Commission

Audit Report

Problem Area 2:

Managing Critical and High Vulnerabilities Older than 30 Days

We found that vulnerabilities older than 30 days were not identified and reported to the Commission’s CIO between January and March 2022. The vulnerabilities were not identified or reported because of a known glitch¹⁷ with how the Tenable.sc software timestamps the date when a vulnerability is first detected by its scan of a system. The OCIO tracks and filters critical and high vulnerabilities older than 30 days using the “First Discovered Date” field in Tenable.sc to measure and manage vulnerabilities.

In order to determine if critical and high vulnerabilities were being patched within the established timeframes, we generated two vulnerability reports from the scanned data available in Tenable.sc, the first on February 14, 2022, and the second on March 7, 2022. The criteria used to generate our two reports included: (1) critical and high vulnerabilities older than 30 days, (2) the first discovered date, (3) the patch published date, and (4) the plugin modification date. The first discovered date is when a vulnerability is first seen on an asset and the plugin modification date is the date when Tenable.sc test criteria for identifying vulnerabilities have been updated.

We discovered vulnerabilities on both reports that were over 30 days old but not reported in the March 2022 executive vulnerability report to the CIO. This occurred because the OCIO did not track the changes in the Tenable.sc’s first discovered date, which altered the age of the vulnerability.

According to the CIO, OCIO divisions were aware of the first discovery date fluctuating and working to identify a solution. In May 2022, the OCIO changed the Commission’s scanning and vulnerability tracking processes to address the date fluctuating problem. Comparing the report

First Discovered Date

The “First Discovered Date” field is the first time that a vulnerability is observed on a system. This date can fluctuate and change if new information is learned about an existing vulnerability. Tenable is aware of fluctuations in the date field and noted that the behavior depends on how Tenable.sc is configured.

Source: <https://community.tenable.com/s/article/Tenable-sc-First-Discovered-Date-Fluctuating>

¹⁷ Tenable addressed the first discovered date fluctuation in a knowledge article on May 20, 2021. In the article, Tenable explained the cause of the fluctuations and provided three alternative configurations clients can use to prevent this from occurring, which are (1) toggling the dynamic host control protocols off for all scans, (2) deploying Tenable agents, and (3) keeping targets in their own repository. See: Tenable SC [First Discovered Date Fluctuating](#)

U.S. International Trade Commission

Audit Report

we generated from Tenable.sc with the February 14 sample we drew from ITCNet, we found 334 critical and high vulnerabilities over 30 days. In the second sample report we generated from ITCNet three weeks later, only 147 of these vulnerabilities were still flagged as over 30 days. We determined that the date changed for 107 of the 147 remaining vulnerabilities. And although the Commission did address exploitable vulnerabilities on ITCNet, bringing the number down from 15 in February 2022 to 3 in March 2022 for the Linux Servers, critical and high vulnerabilities remained.

Table 4 shows the OCIO’s mitigation of vulnerabilities older than 30 days in the two samples we generated over a three-week period. The data in each row show the number of vulnerabilities over 30 days that existed on each system and the severity level of the vulnerabilities. We compared our results from these samples to the Cybersecurity and Infrastructure Security Agency Known Exploited Vulnerability list.

Table 4. Vulnerabilities on the USITC Network Older than 30 days

OIG Sample Taken from ITCNet on February 14, 2022				
Severity Levels	Systems			
	Windows 10	Windows Servers	Linux Servers	Network
Exploitable	0	0	15	0
Critical	9	1	3	0
High	250	4	44	8
Total	259	5	62	8
Grand Total	334			
OIG Sample Taken from ITCNet on March 7, 2022				
Severity Levels	Systems			
	Windows 10	Windows Servers	Linux Servers	Network
Exploitable	0	0	3	0
Critical	2	1	2	0
High	101	1	30	7
Total	103	2	35	7
Grand Total	147			

Source: OIG analysis of ITCNet data on vulnerabilities

U.S. International Trade Commission

Audit Report

After establishing that 147 vulnerabilities from the February 14 report still existed on March 7, 2022, we reviewed the 30-day vulnerability report briefed to the CIO and meeting minutes from March 1, 2022, to determine if these vulnerabilities were tracked and reported. As shown in Table 5 below, the CIO was not kept fully aware of the vulnerabilities. Reviewing the March 1 briefing, we discovered that the CIO was only briefed on 12% of the vulnerabilities. Without an accurate and complete assessment of the age of vulnerabilities, the CIO is not fully informed when deciding how to manage risks related to vulnerabilities.

Table 5. Information on Vulnerabilities Older than 30 Days Reported to the USITC Chief Information Officer on March 1, 2022

Reported to CIO March 1, 2022					
Vulnerabilities Older than 30 Days	System				
	Windows 10	Windows Servers	Linux Servers	Network	Total
Reported to CIO	1	1	16	0	18
Not Reported to CIO	102	1	19	7	129
Total	103	2	35	7	147
Total % Reported to CIO					12%
Total % Not Reported to CIO					88%

Source: OCIO report to Chief Information Officer on March 1, 2022

Vulnerability Management, Commission Policies and Procedures

When vulnerabilities are identified in federal agency information systems, there are a variety of options for handling the vulnerabilities. The Federal Government Cybersecurity Incident and Vulnerability Response Playbooks¹⁸ state that vulnerabilities on a system should be described as:

- **Remediated.** The patch or configuration change has been applied, and the system is no longer vulnerable.
- **Mitigated.** Other compensating controls—such as detection or access restriction—are in place, and the risk of the vulnerability is reduced.
- **Susceptible/ Compromised.** No action has been taken, and the system is still susceptible or compromised.

¹⁸ [The Federal Government Cybersecurity Incident and Vulnerability Response Playbooks](#)

U.S. International Trade Commission

Audit Report

The OCIO's policy on patching is that flaws on the ITCNet are addressed and reported to Network Services, Security Engineering, Service Delivery, and Cyber Security Divisions. It requires critical and high vulnerabilities to be patched within 30 days of first discovery. The CIO relies on accurate information to make risk-based decisions on vulnerabilities older than 30 days. Failure to accurately track existing vulnerabilities could delay resolution and compromise the confidentiality, integrity, or availability of the network.

Recommendation 3: Complete the necessary steps to update the Commission's procedures for the *Vulnerabilities Older than 30 Report* and refine the vulnerability scanning process to accurately track vulnerabilities older than 30 days or adhere to timelines outlined in Binding Operational Directive 22-01 and Binding Operational Directive 19-02.

Management Comments and OIG Assessment

On September 6, 2022, Chairman David Johanson provided management comments on the draft report. He agreed with the findings in the audit that the Commission needs to improve its scanning core infrastructure systems and the management of critical and high vulnerabilities older than 30 days. He also stated that the Commission would provide management decisions to address the three recommendations in the report.

Objective, Scope and Methodology

Objective:

Determine if the Commission is patching critical and high vulnerabilities effectively on ITCNet.

Scope and Methodology

We conducted this performance audit from December 2021 to August 2022 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

U.S. International Trade Commission

Audit Report

We assessed the internal controls relevant to our audit objective. We conducted interviews and reviewed the Commission's data systems and documents to assess risks pertaining to the patching of critical and high vulnerabilities on the International Trade Commission Network. Any applicable weaknesses or deficiencies noted are presented in the audit report. Since our review was limited to internal controls within the scope of our objective, it may not have disclosed all internal control weaknesses that may have existed at the time of this audit.

During our audit, we interviewed OCIO staff, reviewed Commission policies and procedures, and analyzed data from the authoritative hardware list and Tenable.sc. We obtained the list of approved hardware devices authorized to run on ITCNet from the OCIO and reviewed it against the core infrastructure systems scanned by Tenable.sc. We pulled a sample of critical and high vulnerabilities older than 30 days found on systems connected to the ITCNet on February 14, 2022, and compared it to a second sample taken three weeks later on March 7, 2022. The authoritative list and Tenable.sc were used to determine if critical and high vulnerabilities are actively managed, reviewed and prioritized, continuously patched, routinely scanned and reported, and managed and tracked.

We assessed the Commission's core infrastructure vulnerability management program by evaluating the reliability of Windows workstations and servers, Linux servers, and network devices. We also reviewed procedures and interviewed staff knowledgeable in this area. Because the data for Windows 10 systems were incomplete in both the authoritative list and Tenable.sc, we used the data from SCCM and Active Directory to determine if critical and high vulnerabilities were being patched effectively. We also reviewed the 30-day vulnerability report briefed to the CIO on March 1, 2022. We assessed the Commission's major applications collectively rather than individually in the performance of this audit.

U.S. International Trade Commission

Audit Report

Appendix A: Management Comments



UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

C083-UU-001

September 6, 2022

MEMORANDUM

TO: Rashmi Bartlett, Inspector General

FROM: David S. Johanson, Chairman 

SUBJECT: Response to Draft Audit Report – Audit of USITC’s Patching of Critical and High Vulnerabilities on the International Trade Commission Network

Thank you for the opportunity to review and provide comments to the draft audit report – Audit of USITC’s Patching of Critical and High Vulnerabilities on the International Trade Commission Network.

We agree with the audit findings that the Commission needs to improve scanning core infrastructure systems and managing critical and high vulnerabilities older than 30 days. The Commission will develop management decisions to address the three recommendations in the draft report.

U.S. International Trade Commission

Audit Report

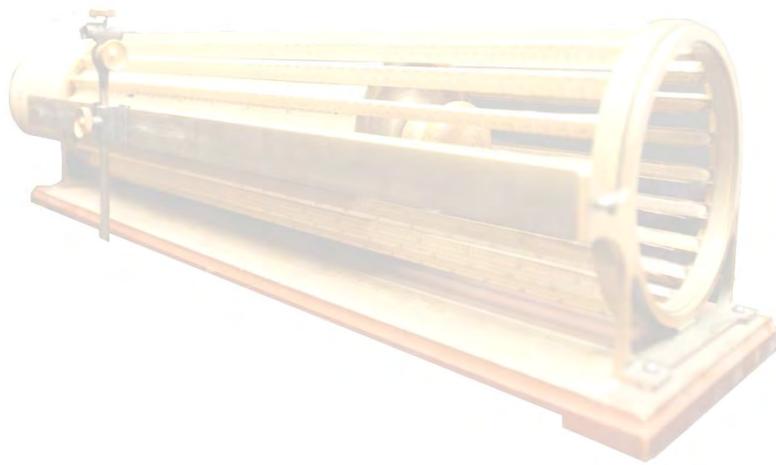
Appendix B

Common Vulnerability Scoring System (CVSS)

CVSS is owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at <https://www.first.org/cvss/>. The CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score that can be translated into a quantitative representation to help organizations properly assess and prioritize their vulnerability management process. The CVSS Base Score ranges from 0.0 to 10.0. The quantitative severity rating for CVSS scores comes from the [National Vulnerability Database](#) (NVD), which is the U.S. government’s repository for vulnerability data. NVD also provides a regularly updated library of common vulnerabilities and exposures (CVEs), providing the rankings and other associated information (such as vendor, product name, version, etc.). The most recent CVSS-related scores and ratings are as follows:

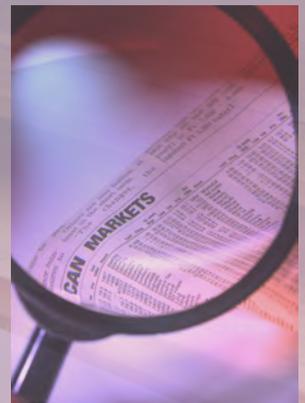
CVSS v3.0 Score	Severity Rating
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

Source: <https://nvd.nist.gov/vuln-metrics/cvss>



“Thacher’s Calculating Instrument” developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to quickly perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission



U.S. International Trade Commission
Office of Inspector General
500 E Street, SW
Washington, DC 20436

Office: 202-205-2210
Fax: 202-205-1859
Hotline: 202-205-6542
OIGHotline@USITCOIG.GOV