TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk

August 28, 2023

Report Number: 2023-20-048

TIGTACommunications@tigta.treas.gov | www.tigta.gov

HIGHLIGHTS: Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk

Final Audit Report issued on August 28, 2023 **Report Number 2023-20-048**

Why TIGTA Did This Audit

Department of Homeland Security's Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (KEV), focuses on vulnerabilities that are active threats and should be Federal agencies' top priority. The directive issued November 3, 2021, required Federal agencies to update internal vulnerability management procedures by January 2, 2022.

In addition, the directive states if an agency is unable to timely remediate a KEV, the agency must remove or isolate the asset from the agency's network.

This audit was initiated to review the IRS's compliance with the directive and whether KEVs are effectively remediated as prescribed.

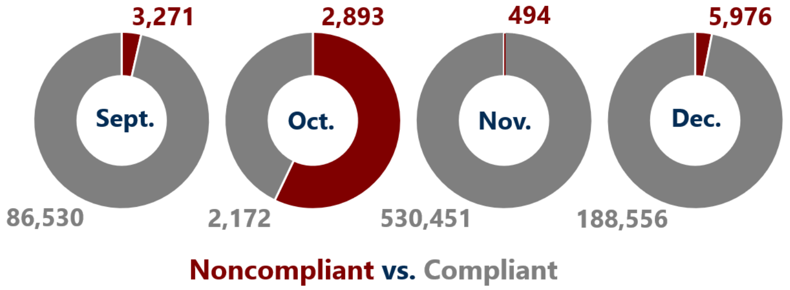
Impact on Tax Administration

The IRS uses its asset and vulnerability repository to track KEVs. Ineffective tracking and untimely remediation of KEVs increase the risk to the overall security of IRS assets and allow affected assets to become targets of external exploitation with the intent to steal taxpayer data. In addition, failure to isolate or remove vulnerable assets from the network increases the risk of malicious attacks.

What TIGTA Found

KEV issues were communicated across the IRS via meetings held regularly, which allowed an opportunity for individuals to discuss relevant issues such as asset vulnerability status, remediation efforts impacting mission-critical assets, asset isolation, and the Virtual Local Area Network isolation pilot effort. In addition, the IRS reported past due unremediated KEVs and mitigation actions to the U.S. Department of the Treasury by completing spreadsheets until the process was automated through the Continuous Diagnostics and Mitigation Federal Dashboard.

From September through December 2022, there were between 494 and 5,976 KEVs past the remediation period.



The repository reflected 91,559 assets with at least one KEV as of December 15, 2022. TIGTA was unable to determine the status of each asset with a KEV because the attack signature change data in the IRS's asset and vulnerability repository are not reliable. In addition, the IRS is not following established guidance to isolate or remove all vulnerable assets from its network.

Further, the directive specifies that Federal agencies are required to track all KEVs from the Cybersecurity and Infrastructure Security Agency's KEV Catalog. However, between September and December 2022, the IRS did not track 14 KEVs. During the audit, the IRS implemented an action to correct this issue. Finally, the IRS's procedures to implement the directive are non-official, draft in nature, and not included in standard operating procedures.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer: 1) timely remediate KEVs in accordance with the directive; 2) immediately isolate or remove assets with KEVs not remediated timely from the network; 3) assess attack signature changes to determine remediation time frames for each and update data in the asset and vulnerability repository; and 4) finalize standard operating procedures and update the Internal Revenue Manual on internal vulnerability management.

The IRS agreed with all four recommendations. The Chief Information Officer plans to timely remediate KEVs in accordance with the Cybersecurity and Infrastructure Security Agency's KEV Catalog, isolate from the IRS network all assets with KEVs not remediated by the established due date, and update procedures.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20024

August 28, 2023

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

Heather Hill

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk (Audit # 202320004)

This report represents the results of our review of the Internal Revenue Service's (IRS) compliance with the Department of Homeland Security's Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, and whether known exploited vulnerabilities are effectively remediated as prescribed. This audit is included in our Fiscal Year 2023 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources*.

Management's complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

According to the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security, the United States faces persistent and increasingly sophisticated malicious cybercampaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy.[1] Vulnerabilities that have been used previously to exploit public and private organizations are a frequent attack vector for malicious cyber actors of all types.

Vulnerabilities could pose significant risk to the Internal Revenue Service (IRS), as malicious actors could seize the opportunity to access these weaknesses within its assets, *e.g.*, information systems, workstations, and desktops, and disrupt operations. Instead of focusing on vulnerabilities that may never be used in a real-world attack, a Department of Homeland Security directive focuses on known exploited vulnerabilities (KEV), which are active threats that should be agencies' top priority.[2] The Cyber Threat Fusion Center (Ctfc) team within the Information Technology organization's Cybersecurity function supports KEV remediation efforts by administering the IRS's directive program.

Results of Review

Known Exploited Vulnerabilities Are Communicated and Reported

The Ctfc team is responsible for developing internal vulnerability management procedures and communicating to the business units expectations on remediation reporting and isolating assets. The Ctfc team hosts status update meetings with personnel from the Information Technology organization and other business units about ways to improve overall vulnerability issues. According to Ctfc management, weekly status meetings were held from February through July 2022, and biweekly status meetings were held from August 2022 to the present. We reviewed documentation from biweekly status meetings held during February and March 2023. Our review of the documentation determined meetings were held regularly and included input from attendees. The meetings allowed an opportunity for individuals to discuss relevant issues such as asset vulnerability status, remediation efforts impacting mission-critical assets, asset isolation, and the Virtual Local Area Network isolation pilot effort.

According to Ctfc management, prior to January 2023, the Department of the Treasury (hereafter referred to as the Treasury Department) would provide the IRS with a spreadsheet template populated with KEV identification numbers. The IRS would then add to the spreadsheet information on its unremediated vulnerability status and send the spreadsheet to the Treasury Department monthly. The data in the spreadsheets are derived from the IRS's asset and vulnerability repository. The spreadsheets provide a status of the IRS's past due

[1] See Appendix IV for a glossary of terms.

[2] The CISA's Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (Nov. 2021).

unremediated KEVs, mitigation actions such as a plan of action and milestones or a risk-based decision to accept the risk to the network, and estimated remediation dates. The Treasury Department was responsible for reporting spreadsheets to the CISA because the IRS does not communicate directly with the CISA about its information technology asset vulnerability status. We reviewed the spreadsheets from February through December 2022 and determined that the IRS completed the spreadsheets for the Treasury Department. Ctfc management stated that as of January 2023, the IRS is no longer required to submit spreadsheets to the Treasury Department, and the IRS's unremediated KEV data are now submitted automatically through the Continuous Diagnostics and Mitigation Federal Dashboard. In April 2023, the Ctfc team was granted access to the dashboard, which allows the team to track what is reported. Ctfc management stated that because the dashboard does not allow mitigation actions to be submitted automatically with the unremediated KEV data, the Ctfc team continues to use the spreadsheets to keep the Treasury Department apprised of the IRS's mitigation efforts.

In addition, the IRS is responsible for vendor reporting requirements. We tested assets hosted by a vendor, *i.e.*, a service provider that hosts IRS assets in a third-party environment, such as the Cloud, and determined that those assets were included in the December 2022 spreadsheet reported to the Treasury Department.

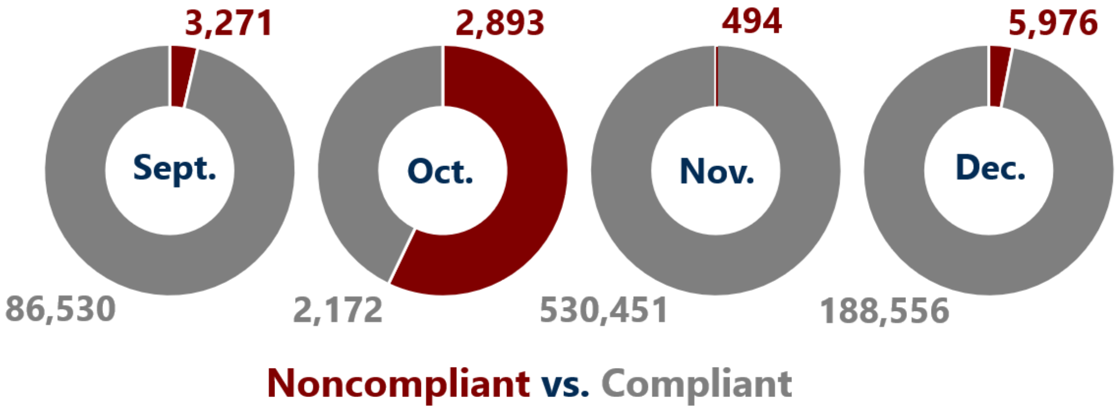
Some Known Exploited Vulnerabilities Are Not Remediated Timely

The directive calls for the timely remediation of all KEVs in accordance with the time frames set forth in the CISA's KEV Catalog.[3] Each KEV has an identification number, a date that it was added to the catalog, and a remediation time frame.

The IRS uses its asset and vulnerability repository to track KEVs. The repository includes the number of days an unremediated KEV has existed on an asset. For September through December 2022, we compared the CISA-established remediation time frame against the number of days a KEV had existed on an asset and found open vulnerabilities on assets past the remediation time frame. During this time, there were between 494 and 5,976 KEVs past the remediation period. Within that population, we identified unremediated KEVs on IRS assets dating back to November 3, 2021. These assets include but are not limited to virtual machines, servers, and user desktops. Figure 1 shows KEVs past due (noncompliant) versus KEVs not past due (compliant). Monthly totals can vary considerably from month to month as new KEV's are identified.

[3] The CISA KEV Catalog contained 824 vulnerabilities in September 2022 and increased to 866 by December 2022.

Figure 1: Unremediated KEVs From September Through December 2022



Source: The IRS's asset and vulnerability repository reports from September through December 2022. Note: an asset may have one or more KEVs.

Information Technology organization management explained that there are numerous reasons vulnerabilities would not be remedied or addressed timely. For example, there may be an existing plan of action and milestones document because a patch may be unavailable. Although the directive states that a vendor must provide clear remediation, *e.g.*, a vendor-provided patch or update, to be included in the CISA's KEV Catalog, Information Technology organization management stated that this does not always occur and some vulnerabilities are added to the catalog with no patch from the vendor. Instead, a vulnerability may be added to the catalog solely because it was exploited. According to CISA management, remediation instructions are provided in the KEV Catalog; however, the Treasury Department should contact the CISA immediately if remediation is not clear.

Information Technology organization management also stated that remediation may be untimely when the vendor requests an upgrade of a product and the remediation action is not a quick patch. Unlike vendor patches, product upgrades require testing such as regression or functional testing, which presents challenges to implementation because the tests are time-consuming. The existence of unremediated KEVs increases the risk to the overall security of IRS assets.

Assets with KEVs were not isolated or removed from the network

The IRS is not following established guidance to isolate or remove all vulnerable assets from its network. Information Technology organization management stated that alternative mitigations such as plans of action and milestones or risk-based decisions are used when assets are not isolated or removed from the network. When a vulnerability cannot be remediated within the directive's time frames and the affected asset is mission critical, *e.g.*, critical to filing season, a plan of action and milestones for mitigation or remediation is developed, or a risk-based decision is used to accept the risk to the network.

However, the directive states that if an agency is unable to timely remediate a KEV, the agency must remove or isolate the asset from the agency's network. According to the CISA, accepting the risk related to a KEV in an alternate mitigation such as a plan of action and milestones or a risk-based decision is not compliant with the directive; as long as an asset is operating and vulnerable, the asset is not compliant.

Non-mission-critical assets

According to Ctfc management, the Treasury Department directed the IRS to document mitigation justifications in the KEV spreadsheet, which alerted Treasury Department officials to affected assets the IRS may have mitigated but did not isolate or remove from the network. Management also stated that there were only two instances when the Treasury Department asked the IRS to remove assets from the network.[4] We reviewed documentation (Cybersecurity function advisories; Knowledge, Incident/Problem, Service Asset Management closed tickets; and a list of the 27 non-mission-critical assets) which showed that of the 1,001 affected assets that were requested for removal from the IRS network, 974 were isolated within four business days, but 27 (2.7 percent) were not isolated. E-mail communication shows all the affected assets that were not isolated or removed from the network were not mission critical for the filing season.

Ctfc management stated that their procedure is to remove from the network unremediated non-mission-critical assets with KEVs. However, e-mail communication revealed instances where Information Technology organization management provided instructions not to isolate or remove non-mission-critical affected assets from the network because KEVs were being worked and the assets needed to remain online to receive upgrades, or that isolation or removal from the network would prolong the remediation time frame.

Failure to isolate or remove vulnerable assets from the network increases the risk of malicious attacks. When affected assets are not isolated, they could become targets of external exploitation with the intent to steal taxpayer data. Removing or isolating affected assets is more effective to reduce taxpayer exposure than other mitigation actions.

2.7% of 1,001 affected non-mission-critical assets we tested were not isolated or removed from the network.

Management Action: In March 2023, we sent an e-mail communication to Information Technology organization executives alerting them to immediately isolate or remove from the network assets with KEVs that are not timely remediated. Information Technology organization executives responded by stating that the IRS recognizes the directive's concerns about isolation and removal of assets, but they also need to ensure that taxpayers can successfully submit individual and business returns during the filing season. Scheduled and unscheduled interruptions to taxpayer availability to complete timely submissions are discouraged. To address both concerns, the Cybersecurity function piloted a process to isolate KEV vulnerable servers and appliances until the assets are remediated successfully to meet the directive's requirement for isolation of devices. According to Ctfc management, as of April 2023, the pilot is ongoing.

[4] The Treasury Department requested the unremediated assets be removed from the network; however, the directive allows for assets to be isolated as well.

The Chief Information Officer should:

Recommendation 1: Timely remediate all KEVs in accordance with the time frames set forth in the CISA's KEV Catalog.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will ensure timely remediation of all KEVs in accordance with the timeframes set forth in the CISA's KEV Catalog.

Recommendation 2: In accordance with the directive, immediately isolate or remove from the network all assets with KEVs not remediated by the established due date.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will implement technology and processes for the ability to isolate from the IRS network all assets with KEVs not remediated by the established due date.

Repository Data Are Not Reliable

The IRS tracks assets with KEVs in its asset and vulnerability repository in an effort to comply with the directive that requires Federal agencies to track all KEVs. To determine whether the IRS is tracking all KEVs in the CISA's Catalog, we compared the IRS's repository to the catalog. From September through December 2022, the IRS did not track 14 unique KEVs. Information Technology organization management stated that they use a manual process to update the repository data, which led to the omissions.

In addition, the IRS did not include any specific data related to the directive's criteria in its repository. For example, there is no data representing accurate remediation due dates of each KEV, time allowed for remediation, or number of days remediation is overdue. Information Technology organization management stated that the data has not been added to the repository because of the large backlog of work within the Cybersecurity function.

We also found data reliability issues caused by not tracking attack signature changes. An attack signature is a pattern or footprint associated with a malicious attack, or an attempt to breach a system, application, network, or device. When this signature is changed, previously remediated vulnerabilities could show as unremediated. However, by prioritizing the addition of data in the repository for the IRS's directive program, the IRS would provide clear evidence of timely remediation prior to signature changes, which would document compliance.

In addition, Information Technology organization management explained that:

- Attack signature change data, *i.e.*, the vulnerability needs an additional patch, are not used consistently. The signature change data may be reflected as the first seen date, *i.e.*, the date the vulnerability is discovered, or the signature change date.
- Attack signature change data are not always applicable to the IRS's affected assets, but management is unable to determine which affected assets are impacted by signature changes.

We analyzed the data in the asset and vulnerability repository. As of December 15, 2022, the repository included 91,559 assets with at least one KEV. We verified that most of the repository data are accurate. For example, the repository accurately identifies asset information such as servers, workstations, and appliances. However, the first seen date and signature change date are not reliable because attack signature change data are not always applicable. As a result, we were unable to determine the timeliness of remediation of the affected assets in the repository.

Attack signature changes create other challenges. For example, Ctfc management stated that there may be instances when the attack signature change comes after the original vulnerability was remediated, but the agency is still held to the original remediation due date to fix the signature change. When this occurs, it appears the IRS is not meeting the directive's requirement to resolve the KEV timely. However, the IRS may have met the original vulnerability remediation due date but missed the due date after the signature changed. Ctfc management indicated attack signature changes occur frequently and estimated they occur in 75 percent of the vulnerabilities.

In November 2022, Information Technology organization management met with the Treasury Department's Chief Information Officer to discuss their concerns over the signature change issue in the spreadsheets and offered a solution to help track the signature changes, which entailed the Treasury Department adding data to the spreadsheets to include signature change dates. At the time of our meetings with Ctfc management, the Treasury Department had not replied. In December 2022, Ctfc management sent follow-up correspondence to the Treasury Department reiterating their concerns from the meeting; as of April 2023, the Treasury Department has not responded. Reaching out to the Treasury Department demonstrates the IRS's due diligence in attempting to correct the issue.

While the CISA recognizes agencies need additional time to apply updates to KEVs remediated previously, the directive is silent on signature change remediation time frames. The CISA's KEV Catalog does not reflect due dates for attack signature changes, but the time needed to fix the signature change could take less time to remediate than the original vulnerability. Because the directive does not address signature changes, agencies are left to determine the remediation time frames. In addition, the CISA is not currently tracking attack signature changes as a frequent problem. Ctfc management stated that the attack signature changes occur frequently. Updating signature change data in the asset and vulnerability repository will allow management to evaluate the significance of the signature change problem if it continues to occur in the future.

Management Actions: During the audit, we discussed the issues of the IRS not tracking unique KEVs and including specific data related to the directive's criteria in its asset and vulnerability repository. The IRS implemented corrective actions to address the issues by automating populating the repository with data from the CISA's KEV Catalog and including the remediation due date, the time frame allowed to complete the required action, and the number of days a remediation is overdue data in the repository. We reviewed documentation and communication records to verify the actions were completed.

Recommendation 3: The Chief Information Officer should assess attack signature changes to determine remediation time frames for each, and update data in the asset and vulnerability repository that include signature change dates applicable to KEVs and the remediation time frame allowed for each signature change as assessed.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will ensure that relevant processes and procedures be updated to reflect the applicable date in the asset and vulnerability repository, inclusive of signature changes and associated dates applicable to the KEV and the remediation time frame.

Directive Implementation Procedures Are Not Finalized

The Ctfc team provided us procedures for implementing the directive. However, the procedures were non-official and draft in nature, *i.e.*, no letterhead, official title, version number, IRS function personnel who prepared it, date, table of contents, and executive approval. The interim guidance for the Internal Revenue Manual has been updated but only provides general information.[5] Standard operating procedures give specific instructions on actions and should be updated to reflect procedures on how to implement a policy. The directive instructs agencies to update vulnerability management procedures in accordance with the directive within 60 days of issuance (by January 2, 2022). At a minimum, the procedures should include the directive's Required Action 1, *i.e.,* internal validation, internal tracking, and reporting requirements. According to Ctfc management, the detailed standard operating procedures include isolation procedures not yet finalized because isolation procedures can vary between environments, *e.g.*, production environment, test environment, and sandbox environment, and need to be developed for each environment. Without written procedures developed and maintained timely, the overall effectiveness of internal controls could be weakened by inconsistencies in tasks performed.

Recommendation 4: The Chief Information Officer should finalize standard operating procedures on internal vulnerability management and update the Internal Revenue Manual.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will ensure that standard operating procedures are finalized regarding internal vulnerability management and that the Internal Revenue Manual is updated accordingly.

[5] Internal Revenue Manual, Section 10.8.50, *Information Technology Security, Servicewide Security Patch Management* (Nov. 2020).

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to review the IRS's compliance with the Department of Homeland Security's Binding Operational Directive 22-01, *Reducing the Significant Risks of Known Exploited Vulnerabilities*, and whether KEVs are effectively remediated as prescribed. To accomplish our objective, we:

- Assessed the IRS's asset and vulnerability repository by determining whether the IRS remediated affected assets in accordance with the directive.
- Determined whether affected assets were isolated in accordance with the directive by interviewing Information Technology organization management and reviewing documentation.
- Determined whether the IRS's KEV inventory matches the CISA's KEV Catalog by reviewing tracking tool documentation and comparing the IRS's asset and vulnerability repository to the catalog.
- Evaluated the accuracy of the attack signature change data captured in the asset and vulnerability repository by interviewing Information Technology organization management personnel and analyzing the data to verify the type of data captured in the repository.
- Determined whether the IRS had procedures for implementing the directive by obtaining and reviewing documented procedures.

Performance of This Review

This review was performed with information obtained from the Information Technology organization's Cybersecurity function located in the New Carrollton Federal Building in Lanham, Maryland, and the CISA located in Washington, D.C., during the period October 2022 through June 2023. We conducted this performance audit 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.

Major contributors to the report were Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Jena Whitley, Director; Khafil-Deen Shonekan, Audit Manager; Chanda Stratton, Lead Auditor; Nicholas Reyes, Senior Auditor; and Laura Christoffersen, Information Technology Specialist (Data Analytics).

Validity and Reliability of Data From Computer-Based Systems

We evaluated the asset and vulnerability repository by analyzing the data, including asset information such as servers, workstations, and appliances, to verify that the appropriate type of information was captured and interviewing Information Technology organization management. We verified that most of the repository data are accurate and reliable for purposes of this report.

However, the first seen date and signature change date are not reliable because attack signature change data are not always applicable. As a result, we were unable to determine the reliability of these specific data for purposes of this report.

Internal Controls Methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: policies, procedures, and guidelines related to the directive. We evaluated these controls by interviewing Information Technology organization personnel, interviewing CISA management, reviewing the IRS's directive program documentation, analyzing the IRS's asset and vulnerability repository, and reviewing tracking tool documentation.

Appendix II

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective action will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 91,559 assets with at least one KEV (see Recommendation 3).

Methodology Used to Measure the Reported Benefit:

We analyzed the data in the asset and vulnerability repository. As of December 15, 2022, the repository included 91,559 assets with at least one KEV. We determined that the first seen date and signature change date are not reliable because attack signature change data, *i.e.*, the vulnerability needs an additional patch, may be reflected as the first seen date, *i.e.*, the date the vulnerability is discovered, or the signature change date. As a result, we were unable to determine the timeliness of remediation of the affected assets in the repository.

Appendix III

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF INFORMATION OFFICER

July 27, 2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya,
Acting Chief Information Officer

Kaschit D. Pandya

Digitally signed by Kaschit D. Pandya
Date: 2023.07.27 16:41:56 -04'00'

SUBJECT: Draft Audit Report – Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk (Audit #202320004)

Thank you for the opportunity to review and comment on the draft audit report. The IRS strives to remediate known exploited vulnerabilities (KEVs) to the maximum extent possible. We recently automated the process of tracking KEVs through the *Continuous Diagnostics and Mitigation Federal Dashboard* and continue to invest in a robust vulnerability management practice to effectively manage cyber-related risks.

As noted in the report, decisions about the isolation and removal of assets must be balanced against the need to ensure that taxpayers can successfully fulfill their federal tax obligations. To this end, we take a holistic approach to fulfilling our broad and multi-faceted cybersecurity responsibilities. This approach includes addressing KEVs and mitigating risk in ways that prevent operational disruptions while simultaneously protecting agency assets.

We concur with the four recommendations in the draft report and plan to complete implementation of all corrective actions by December 2024. We also agree with the outcome measure and will address it along with the associated recommendation outlined in our corrective action plan.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Richard Therrien, Director of Cybersecurity Operations, at (240) 613-5262.

Attachment

Attachment

Audit# 202320004, *Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should ensure timely remediation of all known exploited vulnerabilities (KEVs) in accordance with the timeframes set forth in Cybersecurity and Infrastructure Security Agency's (CISAs) KEV Catalog.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will ensure timely remediation of all KEVs in accordance with the timeframes set forth in CISA's KEV Catalog.

IMPLEMENTATION DATE: November 15, 2023

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

RECOMMENDATION 2: The Chief Information Officer should, in accordance with the directive, immediately isolate or remove from the network all assets with KEVs not remediated by the established due date.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will implement technology and processes for the ability to isolate from the IRS network all assets with KEVs not remediated by the established due date.

IMPLEMENTATION DATE: December 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, User and Network Services

RECOMMENDATION 3: The Chief Information Officer should assess attack signature changes to determine remediation time frames for each, and update data in the asset and vulnerability repository that includes signature change dates applicable to KEVs and the remediation time frame allowed for each signature change as assessed.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will ensure that relevant processes and procedures be updated to reflect the applicable date in the asset and vulnerability repository, inclusive of signature changes and associated dates applicable to KEV and the remediation time frame.

IMPLEMENTATION DATE: July 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Attachment

Audit# 202320004, *Known Exploited Vulnerabilities That Remain Unremediated Could Put the IRS Network at Risk*

RECOMMENDATION 4: The Chief Information Officer should finalize standard operating procedures on internal vulnerability management and update the Internal Revenue Manual.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. The Chief Information Officer will ensure that standard operating procedures are finalized regarding internal vulnerability management and that the Internal Revenue Manual is updated accordingly.

IMPLEMENTATION DATE: March 15, 2024

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Cybersecurity

Appendix IV

Glossary of Terms

Term	Definition
Asset	A major application, general support system, high-impact program, physical plant, mission-critical system, personnel, equipment, or a logically related group of systems.
Attack Signature	A pattern/footprint associated with a malicious attack/attempt to breach a system/application/network/device. They can be found within data sequences or headers that match known malware, source network addresses, destination, specific series of packets, *etc*.
Attack Vector	A path or means by which an adversary can gain access to a system to deliver malicious code or exfiltrate information.
Binding Operational Directive	A compulsory direction to Federal, Executive Branch, departments, and agencies for purposes of safeguarding Federal information and information systems. The CISA within the Department of Homeland Security is authorized to develop and oversee the implementation of binding operational directives. Federal agencies are required to comply with directives except for statutorily defined national security systems.
Business Unit	A title for IRS offices and organizations such as the IRS Independent Office of Appeals, the Office of Professional Responsibility, and the Information Technology organization.
Cloud	The use of computing resources, *e.g.*, hardware and software, which are delivered as a service over a network (typically the Internet).
Continuous Diagnostics and Mitigation Federal Dashboard	A means to view customized reports that alerts security personnel to critical cyber risks and vulnerabilities.
Cybersecurity Function	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Cybersecurity and Infrastructure Security Agency	Develops and oversees the implementation of "binding operational directives" and "emergency directives," which require action on the part of certain Federal agencies in the civilian Executive Branch.

Term	Definition
Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog	A CISA maintained list which serves as the authoritative source of vulnerabilities exploited in the wild.
Dashboard	A user interface or web page that gives a current summary of key information, usually in graphic, easy-to-read form, relating to progress and performance.
Department of Homeland Security	The department of the Federal Government that works to improve the security of the United States. Its work includes customs, border, and immigration enforcement; emergency response to natural and manmade disasters; antiterrorism; and cybersecurity.
Filing Season	The period from January 1 through mid-April when most individual income tax returns are filed.
Functional Testing	Testing software based on its functional requirements. It ensures that the program physically works the way it was intended and all required menu options are present.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Internal Revenue Manual	Primary source of instructions to employees relating to the administration and operation of the IRS and contains directions employees need to carry out their operational responsibilities.
Isolate	A form of removal from the network that minimizes direct access to critical software, critical software platforms, and associated data. Depending on an agency's environment, appropriate isolation techniques may include decommissioning, removal of the vulnerable software product, network segmentation, isolation, software-defined perimeters, and proxies.
Knowledge, Incident/Problem, Service Asset Management	An application that maintains the complete IRS inventory of information technology and non–information technology assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications.
Known Exploited Vulnerability	A vulnerability exploited in the wild.
Mission Critical	Vital to the operation of the organization. Describes the applications required to run the day-to-day business.

Term	Definition
Mitigation	Solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems.
Network	An information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.
Patch	A software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component.
Pilot	A limited version (limited functionality or limited number of users) of a system being deployed to discover as well as resolve problems before full implementation.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, milestones in meeting the tasks, and scheduled completion dates for the milestones.
Regression Testing	Testing a program that has been modified to ensure that additional bugs have not been introduced.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
Risk	A potential event or condition that could have an impact or opportunity on the cost, schedule, business, or technical performance of an information technology investment, program, project, or organization.
Risk-Based Decision	A decision made by individuals responsible for ensuring security by using a wide variety of information, analyses, assessments, and processes and by taking the entire posture of the system into account.
Server	A computer that carries out specific functions, *e.g.*, a file server stores files, a print server manages printers, and a network server stores and manages network traffic.
Standard Operating Procedures	A set of step-by-step instructions compiled by an organization to help workers carry out complex routine operations.

Term	Definition
U.S. Department of the Treasury	The Federal agency that manages Federal finances by collecting taxes and paying bills and by managing currency, Government accounts, and public debt. The Department of the Treasury also enforces finance and tax laws.
Virtual Local Area Network	Collection of devices that are partitioned in a group in which group members can be nearby, *e.g.*, in the same building, or in widely dispersed geographic locations. The devices deliver data protection and security to enable confident connectivity and sharing between critical resources.
Vulnerability	Weakness in an information system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat source.

Appendix V

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
Ctfc	Cyber Threat Fusion Center
IRS	Internal Revenue Service
KEV	Known Exploited Vulnerability

**To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at
oi.govpreports@tigta.treas.gov.**

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.