CYBER RISK SUMMARY:
WATER AND WASTEWATER SYSTEMS FISCAL YEAR 2022

Publication: March 2023

Cybersecurity and Infrastructure Security Agency (CISA)

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:AMBER: Limited disclosure, restricted to participants' organizations. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see https://www.us- cert.cisa.gov/tlp.

SCOPE NOTE

CISA's Cyber Risk Summary evaluates data from Water and Wastewater Systems (WWS) entities' internet-accessible information technology (IT) assets enrolled in CISA's Cyber Hygiene (CyHy) Vulnerability Scanning (VS) and Web Application Scanning (WAS) services. Internet-accessible and internal IT asset vulnerability information from CISA Cybersecurity Assessments, as well as open source and industry information, were also evaluated. The period of analysis is fiscal year 2022 (FY22), from October 1, 2021, to September 30, 2022.

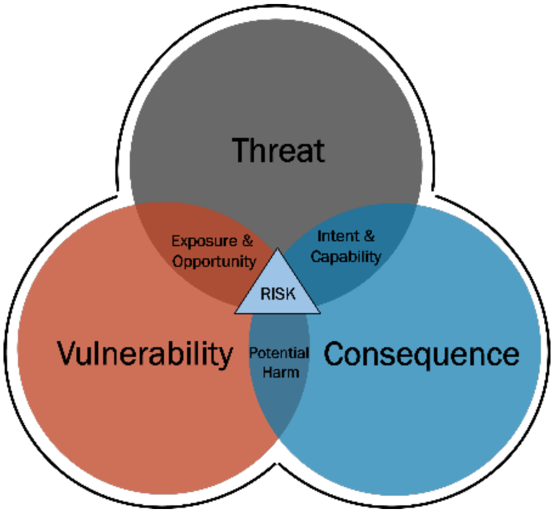
SUMMARY

CISA defines cyber risk as the likelihood that a threat will exploit a vulnerability to cause harm to WWS sector entities through the following means:

- Unauthorized disclosure, modification, or destruction of information.
- Loss of information.
- Loss of system availability.

CISA observed trends of internet-accessible vulnerability exposures belonging to WWS entities that present opportunities for threat actors to employ malicious tactics, techniques, and procedures (TTPs) leveraged in past incidents. Continued exposure to known vulnerabilities or weaknesses almost certainly increases an entity's risk of compromise and adverse consequences for critical functions.

Key Findings*:*



- CISA observed exposure of operational technology (OT)/industrial control system (ICS) assets, including at least one with default credentials, which could impact OT operations and interrupt critical functions.
- Nineteen percent of WWS sector entities exposed known exploited vulnerabilities (KEVs), most of which enable threat actors to execute malicious code directly on a device via the internet. This is known as remote code execution (RCE).
- Ten percent of scanned WWS sector entities ran the Windows 7 operating system (OS). This OS is considered unsupported and has been leveraged to carry out notable cyberattacks against the WWS sector.
- More than a quarter of scanned entities exposed one or more potentially vulnerable services (e.g., Telnet, remote desktop protocol (RDP) on internet-accessible hosts

that, absent compensating or mitigating controls, can provide threat actors with initial access into IT and OT infrastructure.

- Entities enrolled in CISA services exposed outdated versions of software across web applications, which threat actors can leverage to steal data, cause denial of service, and deliver malicious content to an end user.
- Network functionality and device weaknesses, including vulnerabilities in identity and access management, firewall issues, and exposure of unauthorized or unnecessary devices, were observed across WWS sector entities. With the consequent larger attack surface, threat actors can gain greater potential access to WWS sector entities' sensitive systems.
- CISA assessments of WWS entities showed failure of network and endpoint security defenses to stop phishing attempts. This creates opportunities for threat actors to gain initial access to WWS systems.
- Unsupported or insecure encryption was observed across entities, which threat actors are known to target. This increases the risk of leaked credentials, sensitive information disclosure, and account enumeration.
- Newly enrolled WWS sector entities in CyHy VS reduced their active vulnerabilities by an average of 40.7percent within the first three months of enrollment, likely reducing opportunities for exploitation by threat actors.

WWS sector entities should remain vigilant to deter threat activity. CISA recommends that entities consider this analysis in the context of their attack surfaces to decrease opportunity and make it more difficult for threat actors to compromise their networks. CISA recommends WWS entities utilize the mitigations, as mapped to CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) version 1.0, detailed in this report. CISA recommends WWS sector entities also follow EPA's sector-specific guidance. For more detailed mitigations based on findings from the WWS Cyber Risk Summary, please review the Mitigation Companion Report. For more information, contact vulnerability@cisa.dhs.gov.

MITIGATIONS

□ Develop and maintain comprehensive documentation of assets, mapping to the business functions they support and tracking current version information to maintain awareness of outdated software. (CPG 2.3 *Asset Inventory*)

□ Prioritize remediation of vulnerabilities on internet-facing systems within a risk-informed period of time. (CPG 5.1 *Mitigating Known Vulnerabilities*)

□ Implement a phishing awareness training program that includes guidance on how personnel should identify a phishing attack and report both suspected attempts and verified incidents. (CPG 4.3 *Basic Cybersecurity Training*)

□ Strengthen account security to include updated encryption protocols, strong passwords, unique credentials, multifactor authentication (MFA), and the separation of user and privileged accounts. (CPGs 1.1-1.7 *Account Security*)

□ Generally, prohibit exposure of vulnerable services on internet-facing systems. When exposure is necessary, protect the integrity of vulnerable services with compensating controls and maintenance of updated software. (CPG 5.4 *No Exploitable Services on the Internet*)

□ Implement network segmentation to isolate critical systems, namely OT devices, from the corporate network. (CPG 8.1 *Network Segmentation*)

□ Prohibit the exposure of OT assets on the public internet, unless explicitly required for operation. (CPG 5.5 *Limit OT Connections to Public Internet*)

ATTACK SURFACE ANALYSIS

CISA observed trends of internet-accessible vulnerability exposures that present opportunities for threat actors to employ malicious TTPs that have been leveraged against WWS sector entities in past incidents.

Many of the issues identified among WWS sector entities enrolled in CISA's CyHy services are consistent with and carry over from FY21: Internet exposure of OT systems, use of unsupported Operating Systems (OS), outdated software, and exposure of vulnerable services. Enrolled WWS sector entities in FY21 were able to remediate all KEV exposure prior to the end of FY21. However, during FY22, CISA observed longer KEV remediation timeframes along with KEVs persisting at the end of the period of analysis.

CISA observed frequent exposure of outdated versions of software or unsupported OS contributing to vulnerabilities across the sector's attack surface. CISA also detected exposure of vulnerable services known to be leveraged by threat actors to gain initial access and compromise WWS sector entities.

Each WWS sector entity should consider this analysis in the context of its unique environment—specific threats, vulnerability exposure, attack surface, and likely consequence of intrusion—and then create a tailored course of action that reduces cyber risk by limiting threat actor opportunity and increasing difficulty of network compromise.

OT/ICS Internet Exposure Pose Unnecessary Risk of Compromise

According to 2021 CISA reporting,[1] threat actors are known to target OT systems and almost certainly routinely target exposed OT and other ICS devices, such as programmable logic controllers (PLCs).[2] With improperly configured and segmented OT assets, threat actors can:

- Compromise these assets directly.
- Conduct reconnaissance on OT networks.
- Achieve initial access.
- Degrade or disrupt OT and IT operations.

During FY22, CISA observed exposure of OT/ICS assets, such as Modbus service and PLCs. These assets are unlikely to require public internet exposure. If exposed, they provide threat actors with attack surface for a critical WWS asset or system.

- CISA assessments observed exposure of the devices and details of OT technologies residing on IT networks. These OT assets contained information disclosure weaknesses, which could enable threat actors to perform reconnaissance on an entity's OT devices to inform further malicious action. CISA observed at least one OT device configured with default credentials.
- CISA observed exposure of a port that exposed Modbus, an OT service vulnerable to threat actor targeting and exploitation[3] and a PLC device, which threat actors can target for initial access into other connected devices and potential manipulation of safety systems.[4]
- Industry scan data showed a WWS entity exposing a Schneider Electric 171 CBU device, which is a known M1E processor was found, and is known to be vulnerable to CVE-2022-45788. If exploited this can enable arbitrary code execution, denial of service (DoS) and loss of confidentiality and integrity.

[1] "Ongoing Cyber Threat to U.S. Water and Wastewater Systems: Alert Code: AA21-287A," CISA, last modified October 25, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-287a.

[2] "Control System Defense: Know the Opponent: Alert Code: AA22-265A," CISA, last modified September 22, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-265a#:~:text=Execute%20techniques%20and%20tools%20to%20create%20the%20intended%20effects,effects%20on%20the%20target%20system.

[3] Wayne Labs, "Knowing Vulnerabilities In OT Systems Can Help Cybersecurity Efforts," *Food Engineering,* August 26, 2022, https://www.foodengineeringmag.com/articles/100512-knowing-vulnerabilities-in-ot-systems-can-help-cybersecurity-efforts.

[4] Kelly Jackson Higgins, "OT Network Security Myths Busted in a Pair of Hacks," *DarkReading,* February 14, 2023, https://www.darkreading.com/ics-ot/ot-network-security-myths-busted-in-a-pair-of-hacks.

MITIGATIONS

□ Prohibit the exposure of OT assets on the public internet, unless explicitly required for operation. Exceptions must be justified and documented; excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, and mandatory access via proxy or other intermediary). (CPG 5.5 *Limit OT Connections to Public Internet*)

□ Implement network segmentation to isolate critical systems, namely OT devices, from the corporate network. (CPG 8.1 *Network Segmentation*)

KEV Exposure Increases Risk of Exploitation

KEVs are vulnerabilities used by threat actors to actively compromise private and public entities. Entities that expose (or have exposed) KEVs should investigate assets to rule out potential exploitation or compromise. KEVs were identified on nineteen percent of WWS sector entities' networks during FY22.

Sixty-seven percent of observed KEVs could enable threat actors to execute malicious code directly on a device via the internet. This is also known as RCE (MITRE T1203).

CISA maintains a catalog of KEVs that carry significant risk to federal agencies and public and private sector entities.

For the complete catalog, visit cisa.gov/known-exploited-vulnerabilities.

Vendor	KEVs
Apache: Log4j	CVE-2021-44228
Apache: Other	CVE-2020-1938 CVE-2021-40438 CVE-2021-41773
Cisco	CVE-2020-3452 CVE-2020-3580
Microsoft Exchange	CVE-2021-34473
Serv-U	CVE-2021-35247
Spring Framework	CVE-2022-22965

Figure 1. Distinct Active KEVs

- Apache KEVs (CVE-2021-44228 [Log4j], CVE-2020-1938, CVE-2021-40438, and CVE 2021-41773) allow a threat actor to execute arbitrary code, enabling theft of sensitive information, deployment of ransomware, or other malicious activity.[5]

- Microsoft Exchange KEV (CVE-2021-34473) allows a threat actor to execute arbitrary code, enabling theft of sensitive information, deployment of ransomware, or other malicious activity.

KEVs were active on scanned WWS sector entities for a median of 66 days, providing significant windows of opportunity for threat actors to target them and attempt exploitation. At the end of FY22, thirty-three percent of KEVs observed throughout FY22 remained active.

[5] "Apache Log4j Vulnerability Guidance," CISA, last accessed March 14, 2023, https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance.

Use of Unsupported OS Elevates WWS Risk of Compromise

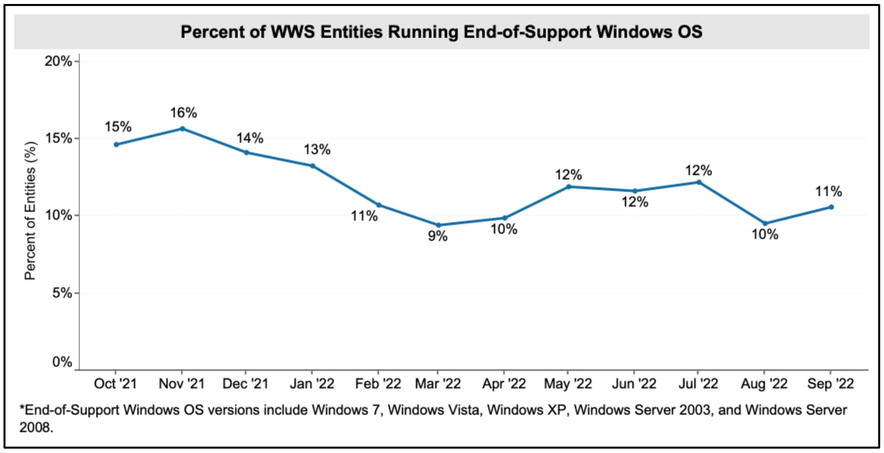


Figure 2. Percent of WWS Sector Entities Running End-of-Support Windows OS

WWSs and devices that are internet accessible and operate with unsupported OS are at increased risk of targeting and exploitation because the vendor will no longer issue formal notifications or updates for newly discovered security issues impacting the OS. Almost one quarter of scanned WWS sector entities exposed unsupported Windows OS.

Continued use of unsupported OS increases threat actors' ability to exploit a system. In 2021, a Florida water treatment plant was compromised through Windows 7, an unsupported OS, which enabled threat actors to leverage associated known vulnerabilities to gain remote access to systems.[6] Up to nine scanned WWS sector entities exposed Windows 7 in FY22.

Note: Windows 8.1 reached end of service on Jan. 10, 2023. At the end of FY22, five WWS sector entities exposed Microsoft Windows 8.1. CISA expects these numbers to increase due to the recent end of support of Windows 8.1.[7]

[6] FBI, CISA, EPA, and MS-ISAC, "Joint Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility – 2021," February 11, 2021, https://www.cisa.gov/uscert/sites/default/files/publications/AA21-042A_Joint%20Cybersecurity%20Advisory_Compromise%20of%20U.S.%20Water%20Treatment%20Facility.pdf

[7] "Windows 8.1 support ended on January 10, 2023," Microsoft, last accessed March 14, 2023, https://support.microsoft.com/en-us/windows/windows-8-1-support-ended-on-january-10-2023-3cfd4cde-f611-496a-8057-923fba401e93.

MITIGATIONS

□ Develop and maintain comprehensive documentation of assets, mapping to the business functions they support and tracking current version information to maintain awareness of outdated software. (CPG 2.3 *Asset Inventory*)

□ Prioritize remediation of vulnerabilities on internet-facing systems within a risk-informed period of time. (CPG 5.1 *Mitigating Known Vulnerabilities*)

□ Collect access and security logs, namely, intrusion detection system/intrusion detection and prevention system (IDS/IDPS), firewall, data loss protection (DLP), and virtual private network (VPN), and ensure logs are securely stored for a direction informed by risk or pertinent regulatory guidance. (CPG 3.1 *Log Collection*, CPG 3.2 *Secure Log Storage*)

□ Maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., business email, web browsing). All privileged accounts should be revaluated on a recurring basis to validate continued need for a given set of permissions. (CPG 1.5 *Separating User and Privileged Accounts*)

Vulnerable Service Exposure Increases Opportunities for Threat Actors

Thirty-one percent of enrolled WWS sector entities exposed vulnerable services that can be leveraged by threat actors to carry out malicious actions.

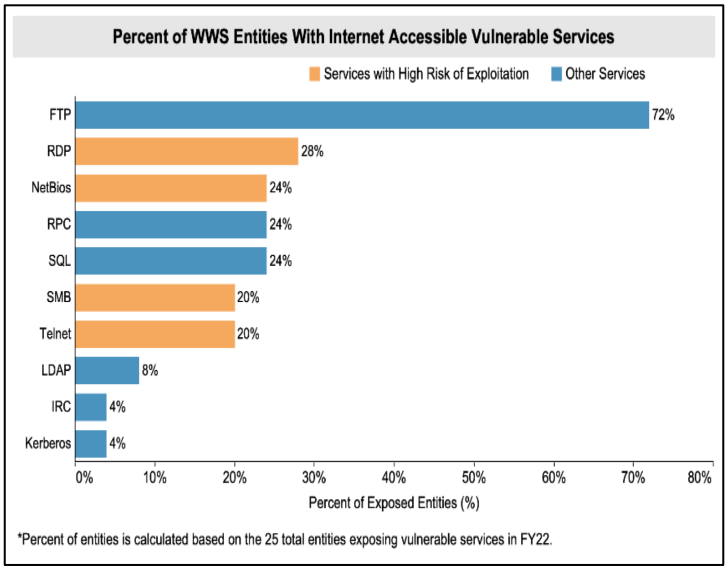


Figure 3. Percent of Entities With Internet-Accessible Vulnerable Services

WWS sector entities exposed remote access services (e.g., RDP) (MITRE T1210) known to be targeted and exploited by threat actors in past incidents within the sector. According to industry reporting, forty-four percent of breaches, including those of Supervisory Control and Data Acquisition (SCADA) systems, were due primarily to vulnerabilities in RDP.[8]

[8] Eduard Kovaks, "SCADA Systems Involved in Many Breaches Suffered by US Ports, Terminals," *Security Week,* October 5, 2022, https://www.securityweek.com/scada-systems-involved-many-breaches-suffered-us-ports-terminals/.

Other remote access services, such as virtual network computing (VNC), were targeted by threat actors. [9]

Several remote access and resource sharing services (e.g., File Transfer Protocol and Server Message Block) identified by CISA enable threat actors to achieve initial access.[10] Exposing publicly accessible services elevates an entity's risk of compromise by enabling public access to systems and functionality within an entity's corporate network.

MITIGATIONS

□ Prohibit exposure of vulnerable services on internet-facing systems except by exception. When exposure is necessary, protect exposure of vulnerable services with compensating controls and maintain updated software. (CPG 5.4 *No Exploitable Services on the Internet*)

□ Implement network segmentation to isolate critical systems, namely OT devices, from the corporate network. (CPG 8.1 *Network Segmentation*)

□ Strengthen VPNs by implementing strong cryptographic and authentication protocols, monitoring user activity for authentication and access attempts, and restricting to only necessary functions. (CPG 3.2 *Secure Log Storage*)

Web Application Security Vulnerabilities Increase Risk of Compromise

Web applications such as JQuery, PHP, Apache, and NGINX accounted for a significant number of the outdated software known to be targeted by threat actors. Web applications represent the most prevalent attack vector leveraged by threat actors in breaches across industries in 2021.[11] The breadth of vulnerabilities exposed across these versions of software could enable RCE, cross-site scripting (XSS), and denial of service, among other actions. All four of these outdated software types have at least proof-of-concept exploit code publicly available for various vulnerabilities.[12]

[9] Water ISAC, "Water Sector Cybersecurity Incident Case Study #004: Ransomware — 2022 SCADA, Brief Impact but Quick Recovery with Standby SCADA Computer – CONT'D," October 24, 2022, https://www.waterisac.org/sites/default/files/%23004-%20Ransomware%20%E2%80%93%202022%20SCADA%2C%20Brief%20Impact%20but%20Quick%20Recovery%20%20with%20Standby%20SCADA%20Computer.pdf
Water ISAC, "Water Sector Cybersecurity Incident Case Study #003: Ransomware — 2021, SCADA, Switched to Manual and Increased Operator Rounds," 2021, https://www.waterisac.org/sites/default/files/%23003-%20Ransomware%20%E2%80%93%202021%20SCADA%2C%20Switched%20to%20Manual%20and%20Increased%20Operator%20Rounds.pdf.

[10] "Weak Security Controls and Practices Routinely Exploited for Initial Access: Alert Code: AA22-137A," CISA, last modified December 8, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-137a.

[11] "2022 Data Breach Investigations Report," Verizon, last accessed March 14, 2023, https://www.verizon.com/business/resources/reports/dbir/.

[12] According to searches performed against VulDB – December 2022

Several WWS sector entities exposed injection and/or XSS (MITRE T1189) weaknesses on web applications and servers. XSS attacks enable a threat actor to use weaknesses in a web application to deliver malicious content to an end user, while injection can lead to data theft, loss of WWS data integrity,[13] denial of service, or system compromise. In 2021, WWS sector entities were targeted by a watering hole attack, a type of XSS, during which an insecure web server/application belonging to a WWS third party was compromised to steal user data.[14] Per industry reporting, most incidents involving web applications can be attributed to the use of stolen or compromised credentials.[15] Injection vulnerabilities exposed by WWS sector entities pose similar risk of compromise to WWS' customers and constituents.

MITIGATIONS

□ Maintain a documented list of relevant threats and cyber actor TTPs and ensure proper detection methods. (CPG 8.2 *Detecting Relevant Threats and TTPs*)

□ Collect access and security logs, namely, IDS/IDPS, firewall, DLP, VPN, and ensure logs are securely stored for a direction informed by risk or pertinent regulatory guidance. (CPG 3.1 *Log Collection*, CPG 3.2 *Secure Log Storage*)

□ Maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., business email, web browsing). All privileged accounts should be revaluated on a recurring basis to validate continued need for a given set of permissions. (CPG 1.5 *Separating User and Privileged Accounts*)

Network Functionality and Device Weaknesses Increase Opportunities for Compromise and Widen Threat Landscape

CISA's data indicated several network functionality and device weaknesses across WWS sector entities' assets and systems, including identity and access management flaws, firewall issues, and exposure of likely unmanaged devices. Observed flaws included weak or easily guessed passwords, presence of default credentials, reused administrative passwords, and insufficient limitation of account privileges, most of which can be leveraged by threat actors to obtain credentials. Although exposure of any of these authentication weaknesses leaves an organization vulnerable, insufficient limitation of account privileges can allow threat actors to utilize accounts with administrative or privileged access to compromise the network (MITRE T1078). Without proper authorization and authentication

[13] NCCoE and NIST, "Securing Water and Wastewater Utilities (Draft)," November 2022, https://www.nccoe.nist.gov/sites/default/files/2022-11/securing-water-and-wastewater-utilities-project-description-draft.pdf.
[14] Ravie Lakshmaman, "Watering Hole Attack Was Used to Target Florida Water Utilities," *The Hacker News,* May 20, 2021, https://thehackernews.com/2021/05/watering-hole-attack-was-used-to-target.html.
[15] "2022 Data Breach Investigations Report," Verizon, last accessed March 14, 2023, https://www.verizon.com/business/resources/reports/dbir/.

practices, WWS sector entities are at risk of network compromise and potential disruption of service.

WWS sector entities exposed outdated versions of Cisco and Pulse Connect software associated with firewall and Virtual Private Network (VPN) functionality for prolonged periods of time. Both types of software are known to be targeted by threat actors, according to CISA's alert on known targeting of Pulse Connect VPN products[16] and Cisco's alert on known attacks against Cisco Adaptive Security Appliance (ASA) vulnerabilities, including two KEVs associated with Cisco ASA and Firepower Threat Defense.[17]

CISA observed that WWS sector entities exposed likely unmanaged devices that provide threat actors with additional vectors for potential compromise. If unmanaged, devices such as printers, Amazon Kindles, or Xbox systems may unnecessarily expand an entity's attack surface.

MITIGATIONS

□ Strengthen account security to include MFA, strong passwords, unique credentials, and the separation of user and privileged accounts. (CPGs 1.1-1.7 *Account Security*)

□ Ensure sensitive data, including credentials, are not stored in plaintext and can only be accessed by authenticated and authorized users. (CPG 3.4 *Secure Sensitive Data*)

□ Monitor user activity and review access logs for unauthorized login attempts and other suspicious activity. (CPG 3.1 *Log Collection*)

Phishing Weaknesses Increase Probability of Threat Actors Gaining Initial Access

CISA observed phishing vulnerabilities in WWS user awareness and in both network and endpoint security defenses. According to open source research, phishing (MITRE T1566) remained a technique favored by threat actors for initial access in 2022.[18] Phishing uses social engineering to either solicit sensitive information through email from targeted users (i.e., user's credentials) or to introduce ransomware or other malware onto user systems and networks. Phishing campaigns leverage a variety of payloads to try to evade both network border and endpoint protections.

[16] "Exploitation of Pulse Connect Secure Vulnerabilities: Alert Code: AA21: 110A," CISA, last modified August 24, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa21-110a.

[17] "Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability," Cisco, last modified October 25, 2022, https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW.

[18] "2022 Data Breach Investigations Report," Verizon, last accessed March 14, 2023, https://www.verizon.com/business/resources/reports/dbir/.

CISA's phishing assessments of WWS sector entities revealed that payloads with the greatest user interaction had subjects referring to company-specific information, followed by notifications for various user accounts. Assessed WWS entities had an average click rate of nearly 13 percent, and up to 32 percent for some entities. It is important to note that threat actors require only one successful interaction for an opportunity to compromise the network.

Most malicious payloads tested by CISA across the WWS sector bypassed network border filters; however, a much smaller set of malicious payloads evaded endpoint protections. CISA observed payloads being successfully deployed via phishing emails, but open-source reporting identified HTML and windows document (doc) files as the most prevalent across sectors.[19] Failure to block phishing payloads can result in many negative outcomes, including disclosure of information for use in follow-on malicious actions or delivery of malware/ransomware resulting in network compromise.

MITIGATIONS

□ Implement phishing-resistant MFA, such as FIDO/WebAuthn application programming interface (API) (CPG 1.3 *Multi-Factor Authentication*)

□ Configure email servers to filter out and block emails with malicious indicators and implement authentication protocols, such as Sender Policy Framework (SPF and DomainKeys Identified Mail (DKIM) to prevent spoofed or modified emails. (CPG 8.3 *Email Security*)

□ Implement a phishing awareness training program that includes guidance on how personnel should identify a phishing attack and report both suspected attempts and verified incidents. (CPG 4.3 *Basic Cybersecurity Training*)

□ Disable macros by default on all devices. If macros must be enabled in specific circumstances, ensure there is policy for authorized users to request that macros are enabled on specific assets. (CPG 2.2 *Disable Macros by Default*)

Poor Encryption Practices Risk Sensitive Data Compromise and Leaks

Encryption protocols ensure that the data is sent by a legitimate source and received at a legitimate destination. Across WWS sector entities, CISA observed the following encryption weaknesses:

- Ninety-six percent of scanned entities were observed with a weakness in their Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol, including use of deprecated versions, use of weak ciphers, or encryption certificate issues.

[19] ESET, "Threat Report T2 2022," We Live Security, 2022, https://www.welivesecurity.com/wp-content/uploads/2022/10/eset_threat_report_t22022.pdf.

- Thirty percent of entities that underwent web application scanning were observed with insecure transport protocols, including unencrypted protocols (HTTP) used for authentication.
- Eleven percent of scanned entities did not enforce use of encryption for their web communications, lacking HTTP Strict Transport Security (HSTS) headers.

Deprecated encryption protocols can allow threat actors to perform network reconnaissance, snooping and intercepting traffic that is not sufficiently protected, and can lead to account credential theft and exfiltration of sensitive data.

MITIGATIONS

□ Update all outdated or weak encryption and maintain properly configured and up to date TLS and encryption protocols. (CPG 3.3 *Strong and Agile Encryption*)

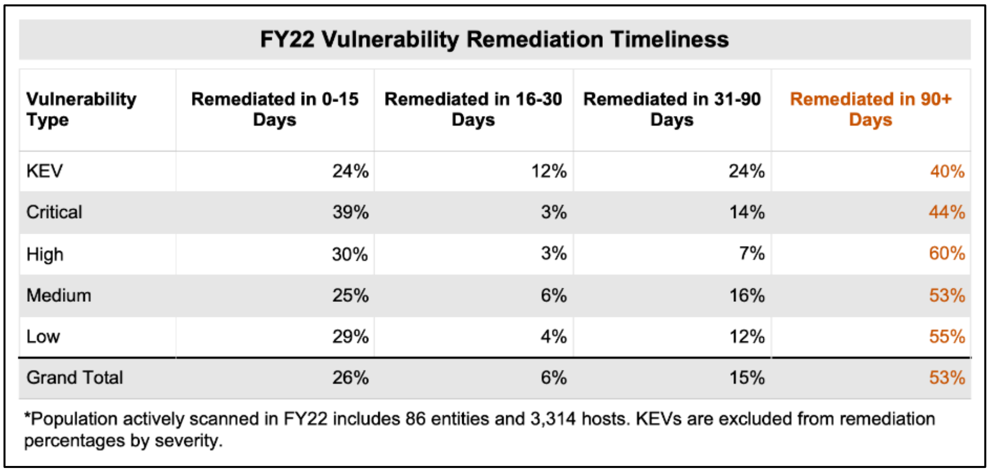
□ Establish and maintain secure configuration baselines for applications and services. (CPG 2.5 *Document Device Configurations*)

VULNERABILITY MANAGEMENT TRENDS

Prolonged Vulnerability Exposures

Prolonged exposure windows increase opportunities for threat actors to identify weaknesses and develop exploitation strategies and capabilities. Analysis of CISA's data indicates that scanned WWS sector entities' responsiveness to address known vulnerabilities and exposures lagged behind CISA's recommended goals for federal agencies. Although WWS sector entities are not required to reach standards of federal agencies, swift remediation or mitigation activities can help to reduce internet-accessible vulnerability, or attack surface, and the risk of compromise. Considerable improvement can be made to reduce vulnerability exposure.

- Sixty-four percent of KEVs took more than 30 days to remediate, indicating most KEVs were remediated outside CISA's recommended time frames, if at all. While CISA provides specific remediation guidance per new KEV added to CISA's KEV catalog, remediation guidance is typically less than 30 days.
- A Log4shell (CVE-2021-44228) KEV that has historically enabled threat actors to gain access, escalate privileges, and maintain a foothold on entity networks was exposed by several entities for a median of 25 days.
- Sixty-one percent of critical and 70 percent of high-severity vulnerabilities took more than 15 and 30 days to remediate respectively, indicating that most WWS sector entity remediations are lagging behind CISA's recommended time frames.



FY22 Vulnerability Remediation Timeliness

Vulnerability Type	Remediated in 0-15 Days	Remediated in 16-30 Days	Remediated in 31-90 Days	Remediated in 90+ Days
KEV	24%	12%	24%	40%
Critical	39%	3%	14%	44%
High	30%	3%	7%	60%
Medium	25%	6%	16%	53%
Low	29%	4%	12%	55%
Grand Total	26%	6%	15%	53%

*Population actively scanned in FY22 includes 86 entities and 3,314 hosts. KEVs are excluded from remediation percentages by severity.

Figure 4. Vulnerability Remediation Timeliness

Vulnerability remediation requirements for federal agencies can be used as a benchmark.

As a best practice, CISA known exploited vulnerabilities should be remediated according to the timelines set forth in the CISA-managed KEV Catalog. Likewise, CISA recommends remediation of all critical and high-severity vulnerabilities identified on internet-accessible hosts within 15 and 30 days, respectively. **Note:** This is required for federal civilian executive branch agencies pursuant to federal directives.

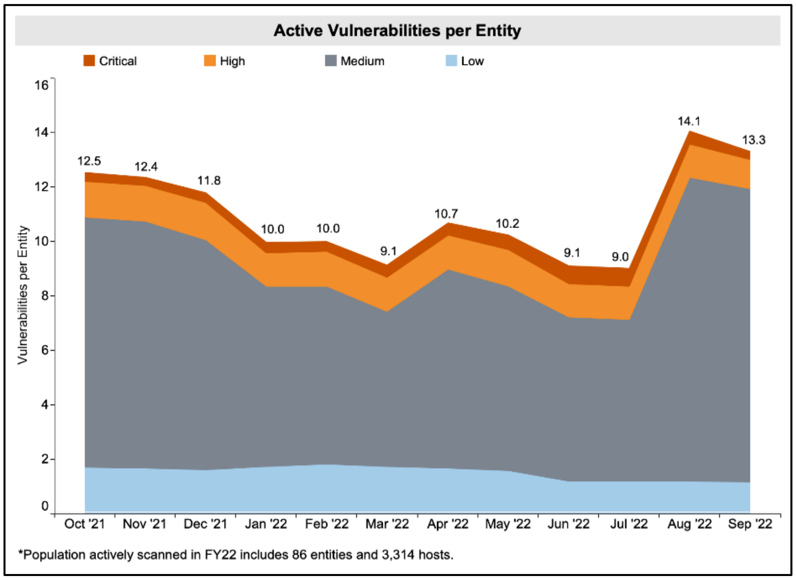
Remediation of Vulnerability Backlog

The average number of active vulnerabilities per scanned entity can provide insight into the WWS sector entities' vulnerability management processes. From October 2021 to September 2022, active vulnerabilities per entity increased slightly, suggesting that WWS sector entities' patching cadence may not have been sufficient to reduce the volume of vulnerabilities that became active on their attack surfaces. Despite a slight increase in active vulnerabilities, WWS sector entities enrolled in CISA's CyHy VS service during FY22 decreased vulnerability exposure by an average of 40.7 percent within the first three months of vulnerability scanning

CISA observed limited remediation from month to month, indicating WWS sector entities could benefit from increased vulnerability management guidance and resources. WWS sector entities remediated on average 18 percent of KEVs and 12 percent of vulnerabilities that were active within each month.

The sudden spike in vulnerabilities exposed per entity from July to August is attributed to a rise in TLS and SSL vulnerabilities. An increase of 84 instances of "TLS Version 1.1 protocol deprecated" and over 120 instances of "SSL certificate cannot be trusted" were observed.

during that period.


Active Vulnerabilities per Entity

*Population actively scanned in FY22 includes 86 entities and 3,314 hosts.

Figure 5. Active Vulnerabilities per Entity

CONCLUSION

WWS sector entities can reduce their cybersecurity risk by following mitigations and recommendations shared throughout this document that are mapped to CISA's CPGs and in a follow-on CISA companion piece. For more support, CISA encourages WWS sector entities to sign up for free CISA services, such as CyHy VS and WAS. WWS sector entities are welcome to seek additional advice and assistance from CISA via vulnerability@cisa.dhs.gov

Feedback regarding this product is critical to CISA's continuous improvement. To submit feedback specific to this product, please use the CISA Product Survey.

APPENDIX A: DATA COLLECTION METHODS AND SERVICES

Data from the following CISA services are analyzed in this report:

CyHy VS tools are deployed to monitor internet-accessible systems for known vulnerabilities, configuration errors, and suboptimal security practices. CISA scans IP addresses with the Nmap network scanner and probes responsive endpoints with the Nessus vulnerability scanner to identify critical, high-, medium-, and low-severity vulnerabilities based on the CVSS v2 scale of 0 to 10.[20] Nessus references the National Vulnerability Database (NVD) for its vulnerability information.[21] The NVD provides CVSS v2 base scores and corresponding severity levels for all Common Vulnerabilities and Exposures (CVEs). Scans use the range of IP addresses provided by the scanned entity. Using these tools, CISA can identify potential and known security issues and can then recommend mitigations to the impacted stakeholder.

CyHy WAS is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, CISA can recommend ways to enhance security in accordance with industry and government best practices and standards.

Cybersecurity Assessments are one-on-one engagements between CISA and an entity that combine national threat information with the vulnerabilities CISA identifies through onsite or remote assessment activities. Assessments may include internet-accessible systems and internal systems. Assessment data derives from one or more of the various CISA offerings, including scenario-based network penetration testing, web application testing, social engineering testing, wireless network testing, configuration management reviews of servers and databases, phishing assessments, and network security architecture reviews. CISA uses security-engineering experts to conduct assessments over a fixed time frame and defines the scope of each engagement by defining IP addresses, system names, and email addresses. At the assessment's conclusion, CISA provides an entity-specific risk analysis report that includes actionable remediation recommendations prioritized by risk. From October 1, 2021, to September 30, 2022, WWS sector entities participated in the following assessments:

> **Risk and Vulnerability Assessments (RVAs)** collect data through assessments and combine it with national threat and vulnerability information to provide an organization with actionable remediation recommendations prioritized by risk. This assessment is designed to identify vulnerabilities that adversaries could exploit to compromise network security controls on internal and external networks.

[20] "Common Vulnerability Scoring System SIG," Forum of Incident Response and Security Teams (FIRST), accessed March 14, 2023, https://www.first.org/cvss.

[21] "National Vulnerability Database," National Institute of Standards and Technology (NIST), accessed March 7, 2023, https://nvd.nist.gov.

Remote Penetration Tests (RPTs) simulate the tactics and techniques used by real-world threat actors to identify and validate exploitable pathways. This service is designed for testing external perimeter defenses, the security of externally available applications, and the potential for exploitation of open-source information.

Phishing Campaign Assessment (PCA) measures a workforce's tendency to click on email phishing lures. Malicious cyber actors commonly use phishing to collect sensitive information or to obtain initial access to a network. Stakeholders can use PCA results to inform the anti-phishing training and awareness that they provide to their workforce.