CYBER RISK SUMMARY: WATER AND WASTEWATER SYSTEMS SECTOR

Publication: March 2022

Cybersecurity and Infrastructure Security Agency

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.

EXECUTIVE SUMMARY

CISA relies on your feedback to improve this product, please fill out the CISA Product Survey.

This Cyber Risk Summary provides analysis, findings, and recommendations derived from non-attributable cybersecurity trends observed during Fiscal Year 2021 (FY21), between October 1, 2020, and September 30, 2021, among 44 Water and Wastewater Systems (WWS) Sector entities enrolled in the Cybersecurity and Infrastructure Security Agency (CISA) Cyber Hygiene (CyHy) Vulnerability Scanning (VS) service that identifies vulnerabilities on internet-accessible information technology (IT) systems that can be exploited by threat actors (Appendix A).

Threat actors likely target the WWS Sector for financial or politically motivated reasons and may attempt to exploit these vulnerabilities. **Note:** WWS Sector entities enrolled in CyHy VS may be aware of the identified vulnerabilities and may have implemented compensating mitigation measures that are not visible to CyHy VS.

CISA's analysis of the available data for 44 scanned WWS Sector entities found:

- By the end of FY21, all identified known exploited vulnerabilities (KEVs) were remediated, likely decreasing risk of compromise of some WWS entities.
- **34.7**% of scanned WWS Sector entities used a potentially exposed risky service, such as Remote Desktop Protocol (RDP), on internet-accessible hosts,[1] which can provide initial access and communication channels for command and control, and data exfiltration.
- **16.3**% of the scanned WWS Sector entities ran unsupported Windows operating systems (OSs)[2] on at least one internet-accessible host by the end of FY21.
- From October 2020, to September 2021, newly enrolled WWS Sector entities in CyHy VS reduced their active vulnerabilities by an average of **37.5**% within the first three months.

CISA recommends the following mitigations to reduce WWS entities risk:

- Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of probable impact.
- Securely configure internet-accessible ports and services on systems and devices by implementing strong identity and access management controls, including strong passwords, multifactor authentication (MFA), and the principle of least privilege.
- Update legacy software and OSs to supported versions in a timely manner and within organizational constraints.
- Segment control system networks and remote devices from organizational network.
- Use the Secure Shell (SSH) Protocol for remote access and virtual private network (VPN).

CISA encourages WWS entities to apply the findings and recommended mitigations in this report as they review their cybersecurity posture and capabilities, conduct further investigations, prioritize actions to mitigate vulnerabilities, and guard against threats. CISA welcomes entities to email vulnerability_info@cisa.dhs.gov for additional advice and assistance.

[1] "Computer Security Resource Center." NIST. Accessed February 10, 2022. https://csrc.nist.gov/glossary/term/host.

[2] Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008 are the only OSs considered unsupported in this analysis.

CONTENTS

SECTOR CYBER RISK OVERVIEW

The WWS is a complex sector composed of drinking water and wastewater infrastructure of varying sizes and ownership types with approximately 153,000 public drinking water systems and more than 16,000 publicly owned wastewater treatment systems in the United States.[3]

Disruptions in WWS services due to the compromise of information technology (IT) and operational technology (OT) systems could impact the availability of safe drinking water (a prerequisite for protecting public health and all human activity), and properly treated wastewater (vital for preventing disease and protecting the environment). Critical services—such as healthcare (hospitals), energy, food and agriculture, and transportation systems that depend on the WWS Sector for safe drinking water and properly treated wastewater—are also likely to suffer negative impacts if WWS services are disrupted. Cyberattacks on WWS entities are likely to affect business enterprise and process control systems—such as treatment and conveyance processes, website and email systems, business enterprise or process control operations—and, potentially, the availability of water and wastewater utilities to provide clean and safe water to customers.[4]

Threat Actors

Threat actors are likely motivated to disrupt the WWS for both geopolitical and financial gain. CISA and its partners have released a joint Cybersecurity Advisory (CSA) that details ongoing cyber threats and malicious cyber activity—by both known and unknown actors—targeting the IT and OT networks, systems, and devices of WWS Sector entities.[5]

The WWS Sector is a target for Advanced Persistent Threats (APTs) and cybercriminals:

- **APTs** may seek to disrupt WWS Sector entities critical functions and economic interests.
  - *In August 2021, malicious cyber actors used Ghost variant ransomware against a California-based WWS [water and wastewater system] facility.*
  - *In September 2020, personnel at a New Jersey-based WWS facility discovered potential Makop ransomware had compromised files within their system.*
- **Cybercriminals** interested in profiting from data breaches and ransomware payments.
  - *In July 2021, cyber actors used remote access to introduce ZuCaNo ransomware onto a Maine-based WWS facility's wastewater SCADA [supervisory control and data acquisition] computer. The treatment system ran manually until restoration of SCADA computer using local control and more frequent operator rounds.*
  - *On May 24, 2021, WSSC [Washington Suburban Sanitary Commission] Water's IT department discovered a ransomware beginning to infect non-essential business systems. WSSC Water successfully halted the virus and removed it within hours.*

[3] "Water and Wastewater Systems Sector." www.cisa.gov. Cybersecurity & Infrastructure Security Agency. Accessed February 10, 2022. https://www.cisa.gov/water-and-wastewater-systems-sector.

[4] "Water Sector Cybersecurity Brief for States." www.epa.gov. United States Environmental Protection Agency. Accessed February 10, 2022. https://www.epa.gov/sites/default/files/2018-06/documents/cybersecurity_guide_for_states_final_0.pdf.

[5] "Ongoing Cyber Threats to U.S. Water and Wastewater Systems." www.cisa.gov. Cybersecurity & Infrastructure Security Agency. Last Modified October 25, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-287a.

It is likely that threat actors targeting and attempted compromise of WWS entities will remain sustained or increased in the short to medium term. Ransomware threat actors seeking financial gain will likely continue to target vulnerable WWS entities, threating the ability of WWS entities to provide clean potable water and effectively manage wastewater. Increased availability of ransomware-as-a-service (RaaS) and the targeting of publicly available vulnerabilities with known exploits are likely to increases risk of compromise for some WWS entities that are unable to adequately invest in cybersecurity or mitigate known vulnerabilities. Although ransomware may initially only impact IT and business networks and applications, it can cause cascading consequences that degrade and interrupt services that other critical infrastructure (CI) sectors depend on.

Vulnerability Compromise

It is likely that some WWS entities are vulnerable to common tactics, techniques, and procedures (TTPs) used by threat actors to compromise IT and OT networks, systems, and devices. WWS entities should be aware of critical vulnerabilities that may exists in their networks and assess their plan to mitigate vulnerabilities that pose significant risk. Threat actors often scan for known, internet facing, vulnerabilities that can provide initial access to networks. For example:

> *In 2021, three incidents of threat actors using ransomware to target supervisory control and data acquisition (SCADA) systems were identified.*[6] *Threat actors likely accessed SCADA systems by exploiting poor password security, outdated operating systems and desktop sharing software. SCADA systems provide monitoring, visibility capabilities and full industrial control system (ICS) for WWS entities. SCADA systems are part of ICS essential to the operation of drinking water utilities. CISA is aware of numerous vulnerabilities affecting OT equipment that may lead to equipment or service disruptions if successfully exploited.*

In light of persistent and ongoing cyber threats, CISA urges critical infrastructure owners and operators, specifically WWS entities, to take immediate steps to strengthen their computer network defenses. CISA encourages leadership at all WWS entities to implement standard cyber hygiene practices to help WWS entities reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

The following analysis provides additional details of known vulnerabilities identified within a sample of WWS entities cybersecurity posture and capabilities. This information can be used to conduct further investigations, prioritize actions to mitigate vulnerabilities, and guard against threats. CISA welcomes entities to email vulnerability_info@cisa.dhs.gov for additional advice and assistance.

[6] Kovacs, Eduard. "Ransomware Hit SCADA Systems at 3 Water Facilities in U.S." October 15, 2021. https://www.securityweek.com/ransomware-hit-scada-systems-3-water-facilities-us

SECTOR VULNERABILITY ANALYSIS AND FINDINGS

Scope and Methodology Note

The following is derived from observations of 44 WWS Sector entities' internet-accessible information technology (IT) assets (1,786 hosts) enrolled in CISA's Cyber Hygiene (CyHy) vulnerability scanning service and 33 cybersecurity assessments conducted from October 1, 2020, and September 30, 2021. The names of specific entities where CISA identified vulnerabilities are not divulged.

Entities enrolled in CyHy VS and those assessed by CISA may not be considered a representative sample of all WWS Sector entities in the United States. CyHy VS provides information on vulnerabilities found on internet-accessible IT systems and does not provide information on compensating controls that entities may employ to reduce the risk of compromise of previously identified or known vulnerabilities. Operational technology (OT) is not assessed or evaluated.

Known exploited vulnerabilities and exposed risky services increase the risk of compromise

Threat actors are very likely to identify and exploit vulnerabilities on entities' internet-accessible IT systems. Throughout FY21, CISA identified 7[7] vulnerabilities on 17 WWS entity networks that are known to be exploited by threat actors to compromise private or public sector organizations. Absent compensating controls, these known exploited vulnerabilities (KEVs) almost certainly increased the entities' risk of compromise through remote code execution (RCE), authentication bypass, and possible denial of service. RCE and authentication bypass vulnerabilities can enable threat actors to execute malicious code directly through the internet on entity systems and allow unauthorized access to files and resources without user authentication. As of the end of FY21, no KEVs that carry significant risk were active on WWS Sector entities, likely indicating that the WWS Sector entities are working to prioritize remediation of vulnerabilities that are known to be exploited.

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

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

Prolonged exposure to KEVs almost certainly increases the opportunity for threat actors to compromise the confidentiality, integrity, or availability of entity networks. The vulnerabilities that are known to be exploited by threat actors were remediated in 41.9 days, which suggests that some entities exposed these vulnerabilities for extended timeframes that, almost certainly increased risk of compromise.

[7] CVE-2019-1653, CVE-2020-17530, CVE-2020-3452, CVE-2021-22900, CVE-2021-26855, CVE-2021-34473, CVE-2021-40539

Threat actors also scan the internet for open ports running vulnerable services that can be compromised. During FY21, 34.7 percent of WWS Sector entities and 2.33 percent of hosts scanned operated potentially risky services[8] exposed to the internet (Figure 1). Operating potentially risky services exposed to the internet likely increases an entity's risk of compromise (see Appendix B). Although some of these services may be used to facilitate legitimate functionality and remote access to systems, they can increase risk if misconfigured or unprotected on internet-accessible hosts. For example, RDP and Server Message Block (SMB) services are known to be targeted by APT and criminal threat actors who, based on CISA reporting, leverage the services to deliver malware variants such as TrickBot and conduct other malicious activity.[9, 10]

In FY21, 8.3 percent of scanned WWS entities ran RDP on at least one internet-accessible host. RDP—which allows remote connection to a computer over a network—is known to be a prime and common vector for ransomware infections, gaining initial access, providing avenues for command and control, and data exfiltration, according to government and industry reporting. It is likely that extensive RDP usage on entity hosts, without compensating controls, increases the risk of compromise by adversaries who leverage RDP as part of their attack path.

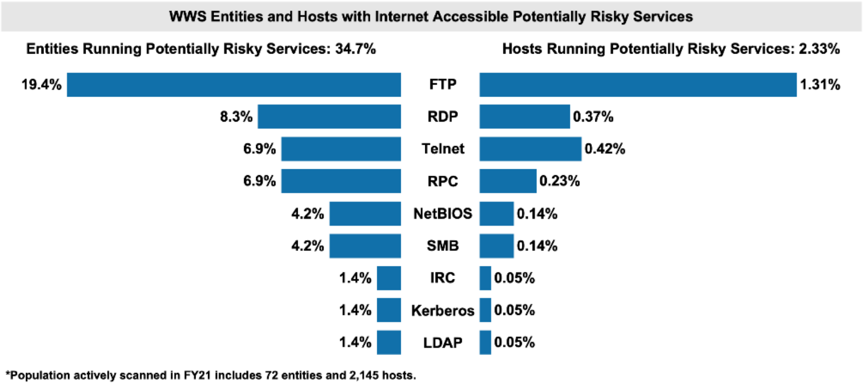


Figure 1: WWS Entities and Hosts Running Risky Services on Open Ports

The most prevalent risky services among scanned WWS Sector entities were File Transfer Protocol (FTP), RDP, and Teletype Network (Telnet) (Figure 1). FTP, identified for 19.4 percent of scanned entities, leverages cleartext communications that are susceptible to password sniffing and eavesdropping attacks. RDP, exposed across 8.3 percent of entities, known to be a prime vector for ransomware infections, gaining initial access, providing avenues for command and control, and data exfiltration. Additionally, Telnet was exposed by almost 6.9 percent of entities and lacks encryption and is susceptible to information disclosure. Entities should be aware of and monitor their use and implementation of these risky services, as their exposure is likely to increase an entity's risk of compromise.

[8] Services, also referred to as network and application protocols, allow devices to send information and communicate over private and public networks, including the internet. When exposed to the internet and unsecured, services are additional entry points for threat actors to launch and orchestrate remote attacks.

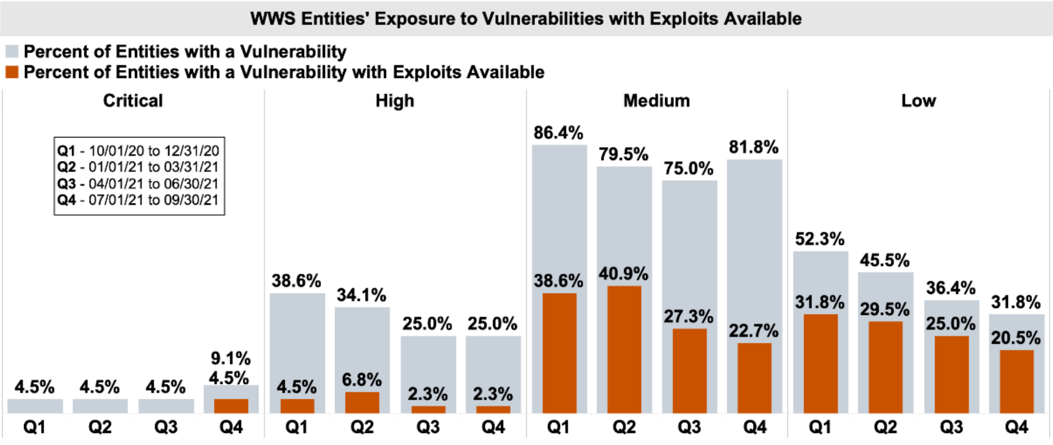
[9] "Alert (AA21-076A)." www.cisa.gov. Cybersecurity & Infrastructure Agency. Last Modified May 20, 2021. https://www.cisa.gov/uscert/ncas/alerts/aa21-076a

[10] "Alert (AA20-296A)." www.cisa.gov. Cybersecurity & Infrastructure Agency. Last Modified December 01, 2020. https://www.cisa.gov/uscert/ncas/alerts/aa20-296a

Vulnerabilities with exploits available pose increased risk to entities

> ***Vulnerabilities with Exploits Available vs. KEVs.***
>
> - *Vulnerabilities with exploits available have a tool, script, and/or malware developed against them that enables a threat actor to engage in exploitation of the vulnerability and potentially compromise entities.*
> - *KEVs are known to be used by threat actors to compromise public and private sector entities, based on reliable evidence.*

Vulnerabilities with publicly available exploits are targeted by a wide array of adversaries as they require fewer resources and provide a higher probability of successfully accessing an entity's network. Entities should prioritize the remediation and mitigation of these vulnerabilities to limit their risk of an adverse cyber event.[11] At the end of the fourth quarter (Q4) of FY21, 4.5 percent of scanned WWS entities had critical severity vulnerabilities with exploits available on at least one host (Figure 2), which, absent compensating controls, likely left those entities at a greater risk of compromise.



*Only entities added prior to FY21 are considered in analysis.

Figure 2: WWS Entities' Vulnerabilities with Exploits Available

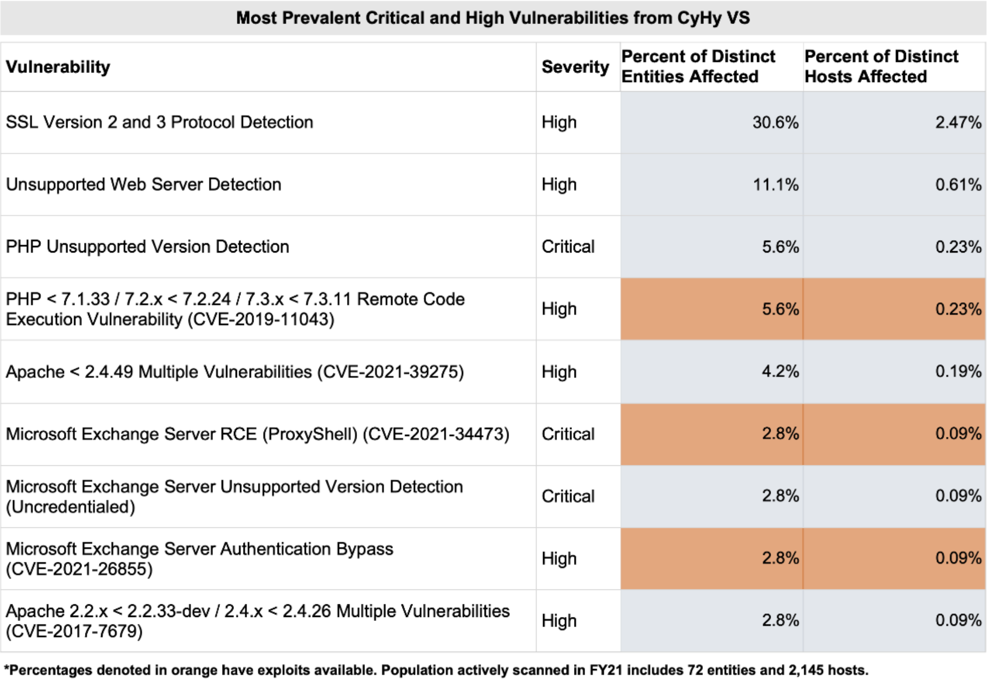
Although a small percentage of hosts may be impacted, critical severity and high severity vulnerabilities with exploits available increase exposure and should be prioritized for remediation. Highlighted below are the most common critical and high vulnerabilities with exploits available among scanned WWS entities:

- Hypertext Preprocessor (PHP) < 7.1.33 / 7.2.x < 7.2.24 / 7.3x < 7.3.11 Remote Code Execution Vulnerability (CVE-2019-11043)
- Microsoft Exchange Server PCE (ProxyShell) (CVE-2021-34473)
- Microsoft Exchange Server Authentication Bypass (CVE-2021-26855)

[11] Spring, et al. "Prioritizing Vulnerability Response: A Stakeholder-Specific Vulnerability Categorization." Carnegie Mellon University Software Engineering Institute. December 19. Accessed February 10, 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379.

Vulnerable, deprecated, and unsupported protocols and operating systems likely common across sector

CISA identified nine critical and high severity vulnerabilities that were prevalent among scanned entities during FY21. Due to their prevalence, it is likely that these vulnerabilities are persistent and can be discovered across the wider WWS Sector (Figure 3). The use of known-weak legacy systems with deprecated, unsupported protocols, software, and OS versions that likely increase threat actor ease of compromise were a commonality among the scanned WWS entities.[12] Unsupported products elevate the vulnerability exposure of a network and provide threat actors with additional attack vectors to leverage in a compromise.



Most Prevalent Critical and High Vulnerabilities from CyHy VS

Vulnerability	Severity	Percent of Distinct Entities Affected	Percent of Distinct Hosts Affected
SSL Version 2 and 3 Protocol Detection	High	30.6%	2.47%
Unsupported Web Server Detection	High	11.1%	0.61%
PHP Unsupported Version Detection	Critical	5.6%	0.23%
PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability (CVE-2019-11043)	High	5.6%	0.23%
Apache < 2.4.49 Multiple Vulnerabilities (CVE-2021-39275)	High	4.2%	0.19%
Microsoft Exchange Server RCE (ProxyShell) (CVE-2021-34473)	Critical	2.8%	0.09%
Microsoft Exchange Server Unsupported Version Detection (Uncredentialed)	Critical	2.8%	0.09%
Microsoft Exchange Server Authentication Bypass (CVE-2021-26855)	High	2.8%	0.09%
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities (CVE-2017-7679)	High	2.8%	0.09%

*Percentages denoted in orange have exploits available. Population actively scanned in FY21 includes 72 entities and 2,145 hosts.

Figure 3: Critical and High Vulnerabilities Detected by CyHy in FY21

The most prevalent vulnerability detected was Secure Sockets Layer (SSL) Version 2 and 3 Protocol Detection (Figure 3).[13] CISA recommends that all WWS Sector entities examine their ingress traffic for deprecated versions of SSL and Transport Layer Security (TLS) and work to remediate or mitigate this vulnerability. Usage of deprecated SSL or TLS Protocols may allow threat actors to gain access to sensitive information on WWS entity networks.[14] Within the WWS Sector, it is also likely that there is a high prevalence of out-of-date PHP and Apache software.

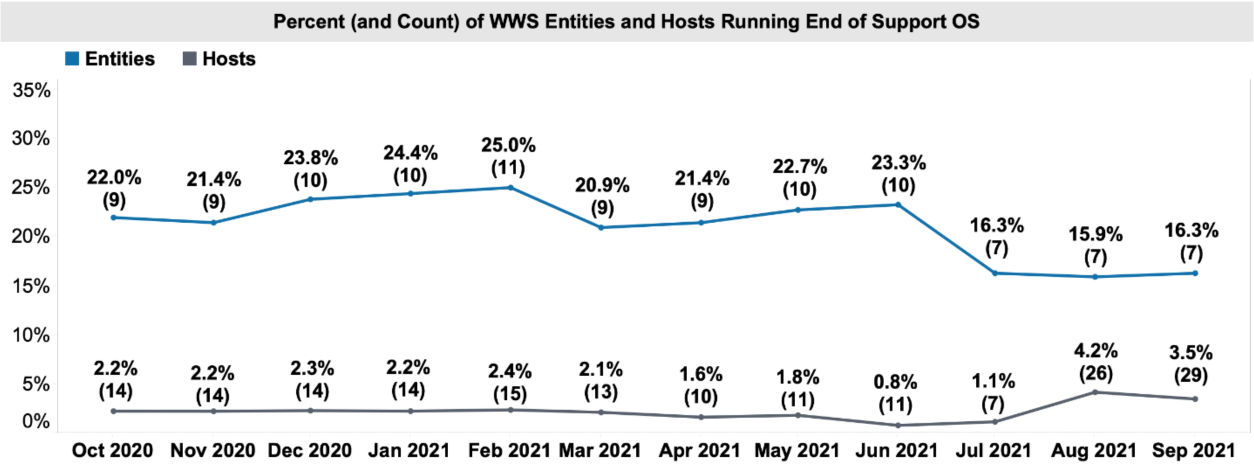
[12] Unsupported software, protocols, and OS versions usually implies that no new security patches for the product will be released by the vendor and, as a result, the product likely contains security vulnerabilities.

[13] The SSL Version 2 and 3 Protocol Detection vulnerability occurs when a remote service accepts encrypted connections using SSL version 2 or 3, both of which are impacted by several cryptographic flaws that can be used by threat actors to compromise the confidentiality and integrity of network communications. SSL is an earlier version of the Transport Layer Security (TLS) cryptographic protocol.

[14] "NSA Releases Guidance on Eliminating Obsolete TLS Protocol Configurations." www.cisa.gov. Cybersecurity & Infrastructure Security Agency. Last Modified January 5, 2021. https://us-cert.cisa.gov/ncas/current-activity/2021/01/05/nsa-releases-guidance-eliminating-obsolete-tls-protocol.

This outdated software introduces vulnerabilities to entity networks, based on a CISA analysis of CyHy VS entities.

At the end of FY21, CISA identified unsupported Windows OS versions (Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008) in seven scanned WWS entities and 29 scanned hosts.[15] CISA's identification of unsupported Windows OSs can indicate that an entity is exposed to additional vulnerabilities as vendors cease software security updates for unsupported products. On February 5, 2021, a water treatment plant in Oldsmar, Florida discovered that threat actors accessed and compromised the plant's system by exploiting unsupported Windows 7 to gain unauthorized access to the system and drastically increased sodium hydroxide levels in the water supply. It is likely that unsupported Windows OS versions increase risk of compromise to some WWS entities.



*Only entities added prior to FY21 are considered in analysis.

Figure 4: Percentage (and Count) of WWS Entities and Hosts Running End of Support OS

Throughout FY21, the percent of entities and hosts running unsupported Windows OS versions decreased by 22.2 percent, which likely indicates that WWS entities are reducing their exposure to vulnerabilities due to unsupported Windows OSs (Figure 4). CISA encourages WWS Sector entities to continue to reduce use and phase out all unsupported OS versions within entity and vendor constraints and stay informed of end-of-support notifications.

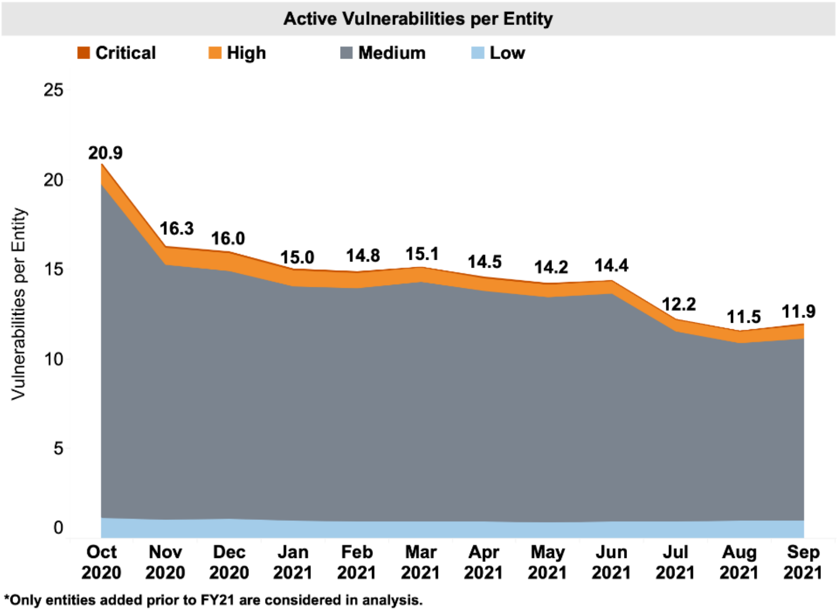
Number of active vulnerabilities per scanned entity declined

The average number of active vulnerabilities per scanned entity can provide insight into the Sector's vulnerability management processes. Remediating more vulnerabilities in each month than the number of new vulnerabilities incurred provides a positive sign that an entity is keeping pace with or reducing active vulnerabilities.

In FY21, newly enrolled WWS entities in CyHy VS reduced their active vulnerabilities by an average of 37.5 percent within the first three months.

[15] Hosts with unknown OS are factored into the overall hosts for the percentage calculation of unsupported OS versions.

During FY21, the number of active vulnerabilities per WWS Sector entity decreased by 43.1 percent, suggesting that entities remediated outstanding internet-accessible vulnerabilities, likely reducing their attack surface and risk (Figure 5).



*Only entities added prior to FY21 are considered in analysis.

Figure 5: Active Vulnerabilities Per WWS Entity

Some vulnerabilities persist, extending opportunity for compromise

CISA examines the number of days a vulnerability remained active before it is remediated as well as the median number of days to remediate vulnerabilities of a particular severity or category to evaluate remediation performance and trends. Prolonged exposure or persistence of vulnerabilities on an entity's network increases the opportunity for a threat actor to leverage a known exploit or develop an exploit, and increases the risk of compromise.

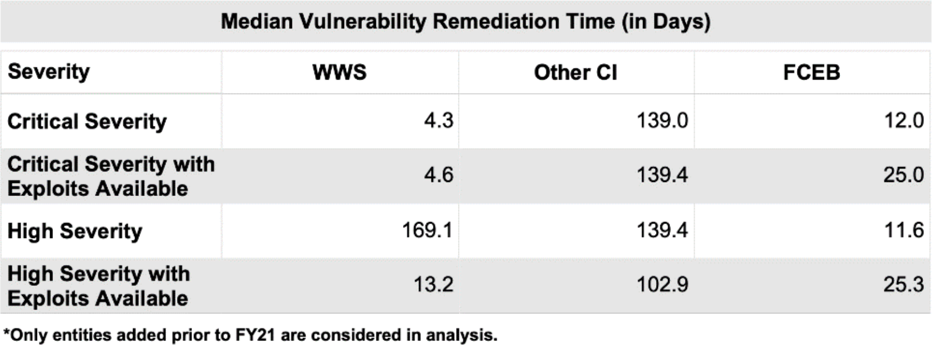
Examining Median Days to Remediate

Examining median days to remediate can signal a need for investigation or modification of vulnerability management processes. Longer remediation times serve as positive and negative indicators of vulnerability management. Median days to remediate will increase as entities address vulnerability backlogs of long-standing vulnerabilities, which is a positive action to reduce risk of compromise. Over time, as this backlog of long-standing vulnerabilities is remediated and a timelier remediation cadence is implemented, entities will likely see a decrease in median days to remediate.

In FY21, 67 percent of all vulnerabilities remediated were open for 30 days or longer (803 out of 1,205), suggesting that, unless compensating controls were in place, entity systems were likely vulnerable for extended periods of time.

Critical and high severity vulnerabilities with exploits available, are highly likely to be targeted by threat actors and pose the greatest risk of compromise. The median days to remediate critical and high vulnerabilities with exploits available is 4.6 days and 13.2 days respectively, which likely indicates that WWS sector entities are remediating vulnerabilities with exploits available in a short period of time and decreasing their exposure and risk of compromise.

Additionally, CISA discovered that 14 percent of all critical severity vulnerabilities and 32 percent of all high severity vulnerabilities were remediated in more than 30 days. WWS Sector entities remediated all critical and high severity vulnerabilities in 4.3 and 169.1 median days, respectively (Figure 6). The median days to remediate critical severity vulnerabilities for WWS Sector entities is 32.2 times faster and high severity vulnerabilities is 1.2 times slower that other critical infrastructure sectors enrolled in CyHy vulnerability scanning.



Median Vulnerability Remediation Time (in Days)

Severity	WWS	Other CI	FCEB
Critical Severity	4.3	139.0	12.0
Critical Severity with Exploits Available	4.6	139.4	25.0
High Severity	169.1	139.4	11.6
High Severity with Exploits Available	13.2	102.9	25.3

*Only entities added prior to FY21 are considered in analysis.

Figure 6: WWS Entities Median Vulnerability Remediation Time Comparison

Assessed entities susceptible to spearphishing and weak password policies

In FY21, CISA performed Remote Penetration Tests (RPTs) and Risk and Vulnerability Assessments (RVAs) for 33 WWS entities and identified 292 findings. 12 percent of findings were critical severity and 30 percent of findings were high severity likely indicating an entity's risk of compromise by malicious actors targeting these vulnerabilities and weaknesses. CISA's findings are categorized by a severity schema described in detail in Appendix C.

57.14 percent of RPTs had critical or high severity spearphishing weaknesses, which were identified through external and phishing assessments (Figure 7).[16] Spearphishing weaknesses likely indicate that assessed entities possessed inadequate border and host-level protections that allowed spearphishing emails to pass through host and network borders and potentially reach a user's inbox. RPTs identify vulnerabilities within the external IP address ranges provided by the assessed entity that could be exploited by an uncredentialed, internet-based user.

[16] RVAs and RPTs assess entities for phishing vulnerabilities, in addition to internal and external network weaknesses.

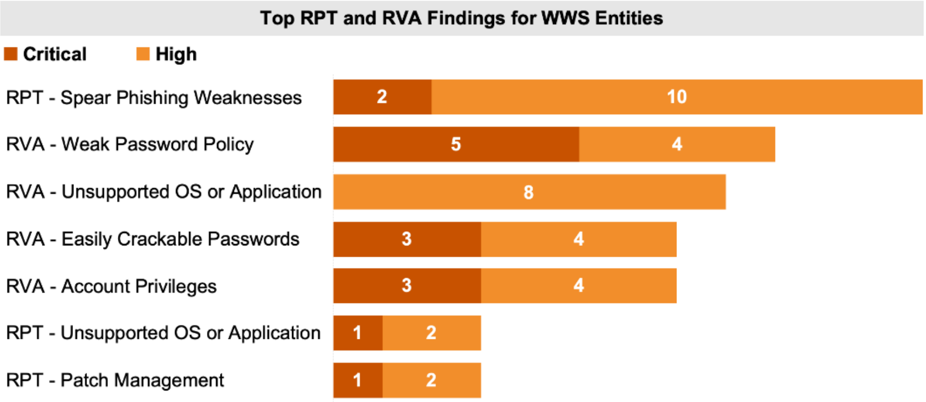


Figure 7: Top RPT and RVA Findings for WWS Entities

In addition to external vulnerabilities, RVAs also identify internal network vulnerabilities that an attacker or disgruntled employee could leverage with their access. 75 percent of RVAs found critical or high severity weak password policy likely indicating that assessed entities allow inadequate password creation susceptible to a variety of attacks including brute force attack. Threat actors regularly initiate attacks by employing brute force attack to forcefully gain access to user accounts.

The next most frequent critical and high severity findings in RVAs include unsupported OS or application, easily crackable passwords, and account privileges.

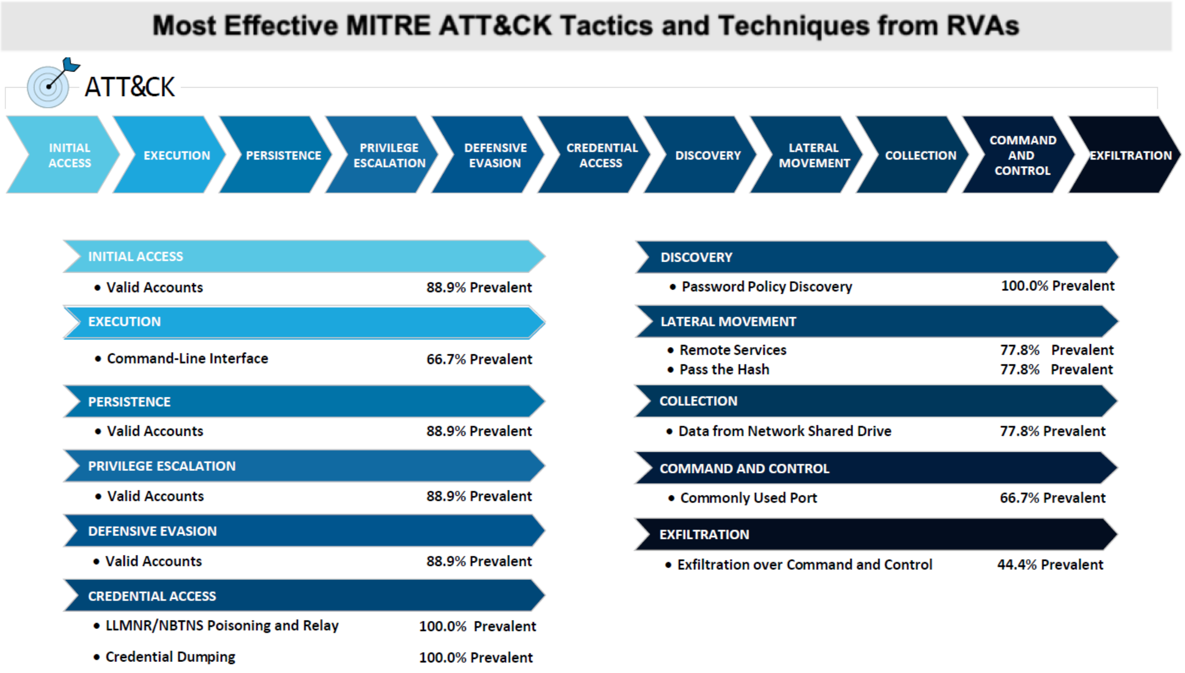
- Failures to move away from using unsupported OSs increases the likelihood of attacks targeting legacy systems.
- Easily crackable passwords may allow a threat actor to gain access to user or administrator accounts, likely increase the entity's exposure.
- Account privileges may allow a threat actor to gain access to multiple systems across a network, likely increase opportunity for entity compromise.

WWS entities could complicate adversaries' ability to attack by applying the latest patches and enforcing complex password policies on internal hosts and systems, based on other frequently observed CISA assessment findings.

RVA attack paths compromising sector systems and networks

During an RVA, CISA assessment teams emulate adversary TTPs to simulate attack scenarios—from initial access to exfiltration—to inform WWS entities of gaps in their defenses. It is likely that threat actors use combinations of successful TTPs to compromise and disrupt victim systems and networks. The MITRE Enterprise Adversarial Tactics, Techniques, and Common Knowledge

(ATT&CK®) framework is used to categorize the success of attempted TTPs observed in RVAs conducted for WWS entities (Figure 8).[17], [18] [19]



INITIAL ACCESS	
• Valid Accounts	88.9% Prevalent
EXECUTION	
• Command-Line Interface	66.7% Prevalent
PERSISTENCE	
• Valid Accounts	88.9% Prevalent
PRIVILEGE ESCALATION	
• Valid Accounts	88.9% Prevalent
DEFENSIVE EVASION	
• Valid Accounts	88.9% Prevalent
CREDENTIAL ACCESS	
• LLMNR/NBTNS Poisoning and Relay	100.0% Prevalent
• Credential Dumping	100.0% Prevalent
DISCOVERY	
• Password Policy Discovery	100.0% Prevalent
LATERAL MOVEMENT	
• Remote Services	77.8% Prevalent
• Pass the Hash	77.8% Prevalent
COLLECTION	
• Data from Network Shared Drive	77.8% Prevalent
COMMAND AND CONTROL	
• Commonly Used Port	66.7% Prevalent
EXFILTRATION	
• Exfiltration over Command and Control	44.4% Prevalent

Figure 8: Successful RVA Tactics and Techniques

Analysis of RVAs suggest that CISA assessment teams were most successful at compromising valid accounts to gain initial access point to obtain credentials to access a range of valid accounts on assessed WWS entities. Initial access typically provides threat actors with a starting point for follow on actions, such as command and control and data exfiltration. By implementing security controls to reduce risk of credential theft on valid accounts, WWS entities may reduce risk of WWS entity compromise and increase adversaries' cost to gaining initial access on entity networks.

WWS entities could further complicate adversaries' ability to attack by applying the latest patches, and enforcing complex password policies on internal hosts and systems, based on other frequently observed CISA Assessment findings.

[17] "CISA Analysis of Risk and Vulnerability Assessments." www.cisa.gov. Cybersecurity & Infrastructure Security Agency. Accessed February 10, 2022. https://www.cisa.gov/publication/rva

[18] "CISA Releases Best Practices for Mapping to MITRE ATT&CK®." www.cisa.gov. Cybersecurity & Infrastructure Security Agency. Accessed February 10, 2022. https://us-cert.cisa.gov/ncas/current-activity/2021/06/02/cisa-releases-best-practices-mapping-mitre-attckr.

[19] The tactics and techniques referenced in this report are from ATT&CK version 8.

MITIGATIONS, AND BEST PRACTICES

The following recommendations and mitigations are based on the analysis and findings of the CISA vulnerability scanning outlined above. CISA provides these recommendations to help WWS Sector entities reduce exposure to vulnerabilities and defend against threats. However, these recommendations do not guarantee protection against all cybersecurity risks impacting the Sector. CISA encourages WWS entities to use these recommendations to review their cybersecurity posture and capabilities, conduct further investigation, and prioritize actions to mitigate vulnerabilities and guard against threats.

CISA recommends entities prioritize remediating vulnerabilities that are known to be actively exploited and have exploits available as quickly as possible.

- *As a best practice—which is required for WWS agencies pursuant to federal directives—CISA strongly recommends remediating all critical and high severity vulnerabilities identified on internet-accessible hosts within 15 and 30 days, respectively.*

Patch Management

Observation: Threat actors scan for and target vulnerable internet-accessible hosts to launch attacks. CISA scanning indicated that 45.5 percent of WWS entities experienced a critical or high vulnerability on at least one internet-accessible host during FY21. The median days to remediate vulnerabilities for WWS entities is 4.3 days for critical vulnerabilities and 169.1 days for high vulnerabilities. In addition, WWS entities' volume of active vulnerabilities per entity decreased from 20.9 to 11.9 in FY21. Entities experiencing a growing vulnerability backlog over time increase the likelihood that one or more of those vulnerabilities are used as part of an attack.

Mitigation:

1. Regularly scan internet-accessible hosts and remediate critical and high severity vulnerabilities within 15 and 30 days, respectively.
2. Continue to reduce the backlog of vulnerabilities, prioritizing those with exploits available that could be used to breach the defensive perimeter. Use CISA's Known Exploited Vulnerabilities Catalog to identify and timely remediate vulnerabilities on WWS entity networks that may pose significant risk of compromise.[20]
3. Prioritize remediation of vulnerabilities using a risk-based approach that considers likelihood of attack, ease of exploitation, and the magnitude of probable impact. Consider remediating active known exploited vulnerabilities first and defining vulnerability prioritization mechanisms that consider contextual factors specific to each entity, such as the SSVC framework.

[20] "Known Exploited Vulnerabilities Catalog." www.cisa.gov. Cybersecurity & Infrastructure Security Agency. Accessed February 10, 2022. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Implementation Resources:

Frameworks and Controls	Technical Guidance	Services
NIST Special Publication 800-40: Guide to Enterprise Patch Management Technologies	CISA: Joint CSA (Ongoing Cyber Threats to U.S. Water and Wastewater Systems)	Sign up for CISA's Cyber Hygiene Vulnerability Scanning
NIST: Critical Cybersecurity Hygiene	CISA Insights: Understand Patches and Remediate Vulnerabilities for Internet-Accessible Systems	Use CISA's Detection and Prevention Services
DHS: Global Infrastructure for Managing Cybersecurity Vulnerabilities	EPA: Develop a Water and utility Training and Exercise Plan	CIS: MS-ISAC Toolkit

Potentially Risky Services

Observation: Threat actors seek to exploit certain services on entities' internet-accessible hosts to gain initial access to entity networks. Certain services like Network Basic Input/Output System (NetBIOS), Telnet, SMB, RDP, and others are vulnerable and are often exploited to deploy malware and move laterally throughout a network. In FY21, 34.7 percent of WWS entities scanned were running at least one potentially risky service on an internet-accessible host.

Mitigation:

1. All listening network ports and services on a system need a validated business reason to run. Entities should identify all internet-accessible services and secure or disable risky services according to the documented business reason for each service to operate.
2. In some cases, operating potentially risky services is necessary and can be accomplished by using additional security measures such as virtual private networks (VPNs), virtual network segmentation, secure credentials and MFA, host-based and network-based firewalls, Transmission Control Protocol (TCP) wrappers or port access control list (ACL) and measures prioritizing secure encryption. It is important to note that many potentially risky services are unique and may require tailored risk assessments to determine an effective risk management approach.

Implementation Resources:

Frameworks and Controls	Technical Guidance	Services
Network Ports, Protocols, and Services: CIS Control 9; NIST CSF PR.IP-1 & DE.WWS-8	NSA's guidance on Eliminating Obsolete Transport Layer Security (TLS) Protocol Configurations	Sign up for CISA's Cyber Hygiene Vulnerability Scanning
NIST Special Publication 800-39: Managing Information Security Risk	MS-ISAC's guidance on How to Restrict Server Message Block (SMB)	CISA's National Cybersecurity Assessments and Technical Services
NIST Special Publication 800-30: Guide for Conducting Risk Assessments	CISA's guidance on Stuff Off Search (S.O.S)	Consider MS-ISACs Albert Network Monitoring service.

Unsupported Operating System Versions

Observation: Threat actors target unsupported OS versions because their lack of security patches and updates increases the ease of exploitation. At the end of FY21, 16.3 and 3.5 percent of scanned entities and hosts, respectively, were running unsupported Windows OS versions.

Mitigation:

1. Entities should maintain a complete software asset inventory that includes the date when software and operating systems will no longer receive support.
2. Entities should identify and plan to allocate resources to replace IT—including software, firmware, OSs, and hardware—that is no longer supported or will reach end-of-support in the near future.
3. For software or operating systems that are unsupported but are required to meet business needs, entities should document exceptions and implement mitigating controls such as network segmentation to isolate vulnerable systems.

Implementation Resources:

Frameworks and Controls	Technical Guidance	Services
Inventory and Manage Software Assets: CIS Control 2; NIST CSF ID.AM-2	MS-ISAC's End-of-Support Software Report List	CISA's Cyber Hygiene Services

CONCLUSION

WWS Sector entities can significantly reduce their cybersecurity risk by performing additional investigation and analysis of the findings described in this report. CISA encourages entities to implement the standard cyber hygiene practices and applicable mitigations identified in this report to reduce their exposure. WWS Sector entities are welcome to seek additional advice and assistance from CISA via vulnerability_info@cisa.dhs.gov and adopt additional best practices from the Water Information Sharing and Analysis Center (WaterISAC).[21]

Feedback regarding this product is critical to CISA's continuous improvement. If you have feedback specific to your experience with this product, please send CISA your input by filling out the CISA Product Survey.

[21] "Water ISAC." www.waterisac.org. Water Information Sharing and Analysis Center. Accessed February 10, 2022. https://www.waterisac.org

APPENDIX A: DATA COLLECTION METHODS AND SERVICES

Data from the following CISA service is 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 hosts with the Nessus vulnerability scanner to identify critical, high, medium, and low severity vulnerabilities based on the CVSS v2 scale of 0 to 10.[22] Nessus references the National Vulnerability Database (NVD) for its vulnerability information.[23] 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.

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 timeframe 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, 2020, to September 30, 2021, WWS 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.
- **Remote Penetration Tests (RPTs)** simulate the tactics and techniques used by real-world adversaries 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 Assessments (PCAs)** evaluate an organization's susceptibility and reaction to phishing emails of varying complexity.

While the entities analyzed in this report do not represent a rigorous statistical depiction of all the complex and varied WWS entities in the United States, CISA encourages all WWS entities to adopt the recommendations and best practices, as applicable.

[22] "Common Vulnerability Scoring System SIG." 2019. FIRST — Forum of Incident Response and Security Teams. 2019. https://www.first.org/cvss/.

[23] NIST. 2019. "NVD - Home." Nist.gov. 2019. https://nvd.nist.gov/.

APPENDIX B: POTENTIALLY RISKY SERVICES

Table 1: Most Common Potentially Risky Services Identified for WWS Entities

Service	Description
FTP	File Transfer Protocol (FTP) is used for the transfer of files between a client and server on a network over a clear-text, or unencrypted, protocol. Cleartext passwords used for authentication are susceptible to sniffing, spoofing, and brute force attacks that can lead to data loss and unauthorized internal network access.
IRC	Internet Relay Chat (IRC) is an unencrypted protocol that facilitates communication in the form of text for group communication. Threat actors may be able to gather sensitive information from IRC communications between users, and launch denial of service attacks on IRC traffic to disrupt user to user interaction.
Kerberos	Kerberos is a computer-network authentication protocol that facilitates communication over a non-secure network in a more secure manner. Unpatched Kerberos connections may allow a threat actor to authenticate onto an entity's network to conduct malicious activity under a legitimate guise.
LDAP	Lightweight Directory Access Protocol (LDAP) is an application protocol that allows clients to perform a variety of operations in a directory server. When exposed to the internet, LDAP could be used by threat actors to gather and manipulate sensitive information related to users, systems, services, and applications on a network.
NetBIOS	Network Basic Input/Output System (NetBIOS) is an unauthenticated protocol that allows applications on computers to communicate over a local area network. When NetBIOS is exposed to the internet, attackers may be able to reach directories, files, and gather sensitive information from devices communicating over the network.
RDP	Remote Desktop Protocol (RDP) allows remote connection to a computer over a network, which can be exploited when misconfigured. RDP should be kept internal to an organization's network and multifactor authentication (MFA) should be used to secure access. Threat actors can use RDP to facilitate data theft and exposure, hijacking login credentials, malware, and ransomware.
RPC	Remote Procedure Call (RPC) enables data exchange and functionality from a different location on the computer, network, or across the internet. Leaving RPC open to the internet may enable threat actors to penetrate the defensive perimeter, exfiltrate data, and modify configurations.
SMB	Server Message Blocks (SMB) is a protocol that provides shared access to files, printers, and serial ports between nodes on a network. SMB lacks support for secure authentication protocols.
SQL	Standard Query Language (SQL) is a standard computer language for managing data held in a relational database, and used to query, insert,

	update, and modify data. Insecure implementations of SQL can be leveraged by threat actors to retrieve sensitive data over database interfaces.
Telnet	Teletype Network (Telnet) is an application protocol used on the internet or local area network for unencrypted text communications. It poses a severe security risk when exposed to the internet, as attackers can see and manipulate the traffic to and from devices with ease.

APPENDIX C: RVA AND RPT SEVERITY RATING CRITERIA

Table 2: Severity Rating Criteria

Severity	Description
Critical	Critical vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploit and potential severe impact. Critical items are reported to the customer immediately.
High	Intruders may be able to exercise full control on the targeted device. Following are examples: • Easily exploitable vulnerabilities that can lead to complete application, system, or network compromise, such as an intruder having the ability to remotely administer files on a web server • Severe router/firewall/server misconfigurations • Worm, Trojan, or backdoor detection • Vulnerability that has tools readily available on the internet to exploit • Weak passwords for remote administration and users
Medium	Intruders may be able to exercise some control of the targeted device. Following are examples: • Disclosure of unauthorized sensitive customer information or user account information • Ability of an intruder to obtain full read access to corporate confidential information • Lack of basic logging and alerting capabilities • Antivirus misconfigurations • Untrusted networks having access to trusted networks
Low	The vulnerabilities discovered are reported as items of interest but are not normally exploitable. Many low-severity items reported by security tools are not included in this report because they are often informational, unverified, or of minor risk.
Informational	These vulnerabilities are potential weaknesses within the system that cannot be readily exploited. These findings represent areas of which the customer team should be cognizant, but they do not require any immediate action.

APPENDIX D: COMMON RVA AND RPT FINDINGS

Table 3: Common RVA and RPT Findings for Scanned WWS Entities

Finding Name	Finding	Standard Remediation
Spearphishing Weakness	Successful spearphishing requires an attacker's email to pass through the network border and execute on the local host with the aid of a user performing some action. Most common phishing attacks can be rebuffed by good border and host-level automated protections. Inadequate protections allow the execution of malicious payloads.	Regularly analyze border and host-level protections, including spam-filtering capabilities, to ensure their continued effectiveness in blocking the delivery and execution of malware.
Spearphishing Susceptibility	Spearphishing attacks use custom-tailored email messages embedded with links or files designed to entice a user to visit a malicious website or download a malicious file, usually resulting in a malware infection or other compromise of the remote host. These attacks are highly effective because they exploit individuals' trusting and gullible nature to trick them into compromising their own systems.	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from a suspicious email or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller. Targeted training should be provided to those who fall victim to the exercise.
Patch Management	Patches and updates are released to address existing and emerging security threats and address multiple levels of criticality. Failure to apply the latest patches can leave the system open to attack with publicly available exploits.	Enforce consistent patch management across all systems and hosts within the network environment. Where patching is not possible due to limitations, implement network segmentation to limit exposure of the vulnerable system or host. Deploy automated patch management tools on all systems for which such tools are available and safe.

Finding Name	Finding	Standard Remediation
Easily Crackable Passwords	User account passwords on the system are common and widely used. An attacker can iterate through a wordlist to successfully predict the victim's password and gain access to the account.	Enforce user creation of strong/unique passwords in accordance with applicable federal standards, industry best practices, and/or agency-defined requirements.
Unencrypted Transmission of Sensitive Information	Unencrypted transmission of data allows an attacker to intercept traffic between two systems or endpoints and recover any information traversing the channels in cleartext. Usernames and passwords are some of the types of data that can be obtained by passing unencrypted data across the network.	Configure systems and applications to use encrypted communications mechanisms that comply with applicable federal standards, industry best practices, and/or agency-defined requirements.
PII Disclosure	One or more applications, systems, or databases disclosed personally identifiable information (PII) to unauthorized users. PII is information that can be used to verify a person's identity, such as Social Security Number (SSN) or credit card numbers. Refer to NIST SP 800-122 as a reference for PII definition.	Implement a process to review files and systems for insecure handling of PII. Properly secure or remove the information. Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in cleartext.
Authentication Bypass	Authentication bypass exists when an application employs weak or broken mechanisms to verify a user's identity before granting that user access to protected functionalities. Authentication bypass can enable an attacker to access an application and utilize its resources and functionality to perform unauthorized operations.	Disable any service that is vulnerable to authentication bypass. If the service cannot be disabled, isolate the service within the network to limit the effectiveness of any bypass. Ensure that only ports, protocols, and services with validated business needs are running on each system.

Finding Name	Finding	Standard Remediation
Insecure Default Configuration	Default configurations of systems, services, and applications can permit unauthorized access. Many off-the-shelf applications are released with built-in administrative accounts using predefined credentials that can often be found with a simple web search. As a result, an attacker with minimal technical knowledge can then use these credentials to access the related services.	Review all vendor applications and appliances. Verify the implementation of appropriate hardening measures, and change, remove, or deactivate all default credentials. Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
Unsupported OS or Application	Using software or hardware that is no longer supported by the vendor poses a significant security risk because new and existing vulnerabilities are no longer patched. There is no way to address security vulnerabilities on these devices to ensure that they are secure. This puts the overall security posture of the entire network at risk because an attacker can target these devices to establish an initial foothold into the network.	Evaluate the use of unsupported hardware and software and discontinue where possible. If discontinuing the use of unsupported hardware and software is not possible, implement additional network protections to mitigate the risk.