CYBER RISK SUMMARY:
FINANCIAL SERVICES (FS) SECTOR 2022

Publication: April 2023

Cybersecurity and Infrastructure Security Agency (CISA)

SCOPE NOTE

CISA's Cyber Risk Summary (CRS) evaluates data from FS entities' internet-accessible information technology (IT) assets enrolled in CISA's Cyber Hygiene (CyHy) Vulnerability Scanning (VS) and Web Application Scanning (WAS) services. CISA evaluated the Internet-accessible and internal IT asset vulnerability information from CISA Cybersecurity Assessments, as well as open source and industry information. The period of analysis is calendar year 2022 (CY22), from January 1, 2022, to December 31, 2022.

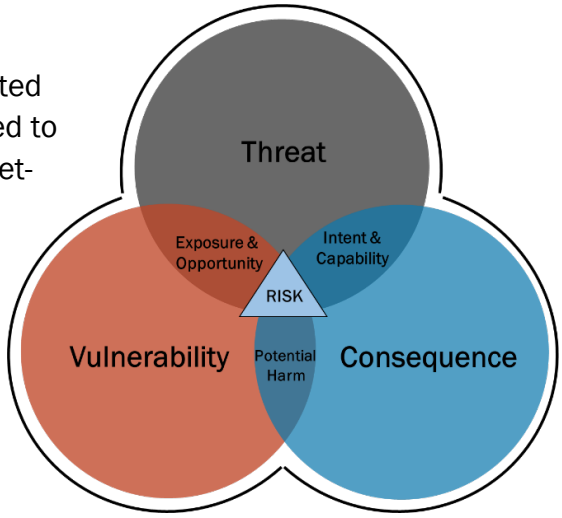
SUMMARY

CISA defines cyber risk as the likelihood that a threat actor will exploit a vulnerability to cause harm to the FS sector through:

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

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

Key Findings:



- Twenty-six distinct entities exposed Known Exploited Vulnerabilities (KEVs), that threat actors have used to compromise public and private entities, on internet-facing assets.
- At least 109 scanned entities had vulnerabilities on scanned web applications that could provide threat actors with a variety of opportunities for exploitation that may enable access to sensitive information or affect FS customers.
- Scanned and assessed entities had protocols and policies that could allow malicious actors to exploit encryption weaknesses, enumerate FS systems, and negatively impact operations.
- Over half of scanned FS entities ran outdated or unsupported software, which threat actors can leverage to steal data, cause denial of service, and deliver malicious content to end users.
- Roughly 10% of scanned entities exposed Windows Operating System (OS) versions that are no longer supported with patches or security updates, increasing exposure to vulnerabilities that can enable full system compromise.
- At least 12% of entities exposed one or more 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 operational technology (OT) infrastructure.

- FS entities participating in CISA assessments blocked 40% of phishing payloads at the border and 90% at the endpoint level, indicating there are weaknesses in network and endpoint security defenses that remain vulnerable to phishing campaigns.
- FS entities enrolled in CISA's CyHy VS service during CY22 decreased vulnerability exposure by an average of 20.1% within the first three months of conducting vulnerability scanning.

FS sector entities must remain vigilant to deter threat activity. CISA recommends that entities consider this analysis in the context of their attack surfaces to decrease opportunities and make it more difficult for threat actors to compromise their networks. CISA also recommends FS entities use the mitigations, mapped to CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), throughout this report. For more information, please contact vulnerability@cisa.dhs.gov.

Mitigations

- ☐ Develop and maintain comprehensive documentation of assets—tracking current version information to maintain awareness of outdated and unsupported software. (CPG 1.A *Asset Inventory*)
- ☐ Prioritize remediation of known vulnerabilities on internet-facing systems within a risk-informed period of time. (CPG 1.E *Mitigating Known Vulnerabilities*)
- ☐ Strengthen account security to include updated encryption protocols, strong passwords, unique credentials, phishing-resistant multifactor authentication (MFA), and the separation of user and privileged accounts. (CPG 2.K *Strong and Agile Encryption*, CPG 2.A *Changing Default Passwords*, CPG 2.B *Minimum Password Strength*, CPG 2.C *Unique Credentials*, CPG 2.H *Phishing-Resistant Multifactor Authentication (MFA)*, and CPG 2.E *Separating User and Privileged Accounts*)
- ☐ 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 2.I *Basic Cybersecurity Training*)
- ☐ Prohibit exposure where possible 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 2.W *No Exploitable Services on the Internet*)
- ☐ Implement network segmentation to isolate critical systems, namely OT devices, from the corporate network. (CPG 2.F *Network Segmentation*)
- ☐ Prohibit the exposure of OT assets on the public internet unless explicitly required for operation. (CPG 2.X *Limit OT Connections to Public Internet*)

ATTACK SURFACE ANALYSIS

CISA observed trends of internet-accessible vulnerability exposures belonging to scanned FS entities that present opportunities for threat actors to employ malicious TTPs that have previously been leveraged against FS entities.[1]

Scanned entities within the FS sector saw some positive trends throughout the calendar year, such as fewer exposed distinct KEVs when compared to CY21 analysis. However, many of the issues identified among FS entities enrolled in CISA's CyHy services, such as long KEV exposure windows, weaknesses in web applications, use of unsupported operating systems, and exposure of vulnerable services are consistent with and carry over from previous analysis periods.

Entities in the FS sector should consider this analysis in the context of their individual threats, vulnerability exposure, attack surface, and likely consequences to inform courses of action aimed at reducing cyber risk by limiting opportunities and increasing difficulty for threat actors to compromise their networks.

KEV Exposure Increases Opportunity for Exploitation

KEVs[3] are common vulnerabilities and exposures (CVEs) that are known to have been actively exploited by threat actors to compromise public and private entities. Analysis of CISA data identified 26 distinct FS entities (documented in Figure 1) exposing at least one of six KEVs on internet-facing assets associated with versions of software from Apache (including Log4j), Cisco, and PHP during CY22. The Log4j vulnerability has historically enabled threat actors to gain access to entity networks and is one of the top routinely exploited vulnerabilities during the period of analysis.[4] CISA recommends organizations keep all software up to date, prioritize patching of KEVs, and minimize attack surface where applicable to decrease the likelihood of agency network compromise.

VENDOR	CVE
Apache	CVE-2021-40438 CVE-2020-1938 CVE-2021-44228/VMSA-2021-0028[2]
Cisco	CVE-2020-3452 CVE-2020-3580
PHP	CVE-2019-11043

Figure 1: Distinct Active KEVs

- Apache KEVs (CVE-2021-40438, CVE-2020-1938, and CVE-2021-44228/VSMA-2021-0028 (Log4j)) allow for Server-Side Request Forgery (SSRF), remote code execution (RCE), and improper privilege management exploits. A threat actor can leverage these vulnerabilities to gain remote access into a machine or network, access privileged data and applications, and create forward requests to arbitrary servers. This allows actors to obtain, modify, or delete resources that would

[1] Note: This Analysis Uses The MITRE ATT&CK® for Enterprise Framework, Version 12.
[2] This CVE and VMWare notation is associated with Log4j, which is a widespread exploitation of a critical remote code execution. Please review CISA's guide on management/remediation. *CISA*, https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance.
[3] CISA maintains a catalog of KEVs that carry significant risk to federal agencies and public and private sector entities. *CISA*, cisa.gov/known-exploited-vulnerabilities.
[4] Dalibor Gasic, "Top 10 Most Exploited Security Vulnerabilities In 2022 (And How To Fix Them)," *PurpleSec*, December 16, 2022, https://purplesec.us/security-insights/top-vulnerabilities-2022/.

otherwise be inaccessible, and enable the compromise of sensitive information.

- Cisco Adaptive Security Appliance KEVs (CVE-2020-3580, CVE-2020-3452) can enable cross-site scripting (XXS) (MITRE T1189) and cause cryptographic collisions. This results in the attacker being able to bypass access controls and impersonate an affected target device to decrypt and exploit a user's personal key.
- PHP KEV (CVE-2019-11043) can lead to data loss, system disruption, deployment of ransomware, and access to other sensitive systems through RCE.

Mitigations

- ☐ Prioritize remediation of known vulnerabilities on internet-facing systems within a risk-informed period of time. (CPG 1.E *Mitigating Known Vulnerabilities*)
- ☐ Monitor user activity and review access logs for unauthorized login attempts and other suspicious activity. Ensure logs are securely stored for a direction informed by risk or pertinent regulatory guidance. (CPG 2.T *Log Collection*, CPG 2.U *Secure Log Storage*)
- ☐ Update all outdated or weak encryption and maintain properly configured and up to date TLS and encryption protocols. (CPG 2.K *Strong and Agile Encryption*)

Web Application Weaknesses Known to be Targeted by Threat Actors

Exploitations of vulnerabilities in FS sector web applications can have a significant impact on the confidentiality, integrity, and availability of data and services critical to the function of the FS sector and the trust of their customers. The FS sector is an attractive target to threat actors for financial gain, and it has a large attack surface because many of its services must be internet-accessible to its customer base via web applications. Vulnerable web applications present attackers with opportunities to use common TTPs including lateral movement, privilege escalation, and data exfiltration. A system compromise can result in costly downtime, loss of customer confidence, and a potential detrimental impact on the global economy.

Figure 2 presents WAS vulnerabilities broken down by Open Worldwide Application Security Project (OWASP) category.

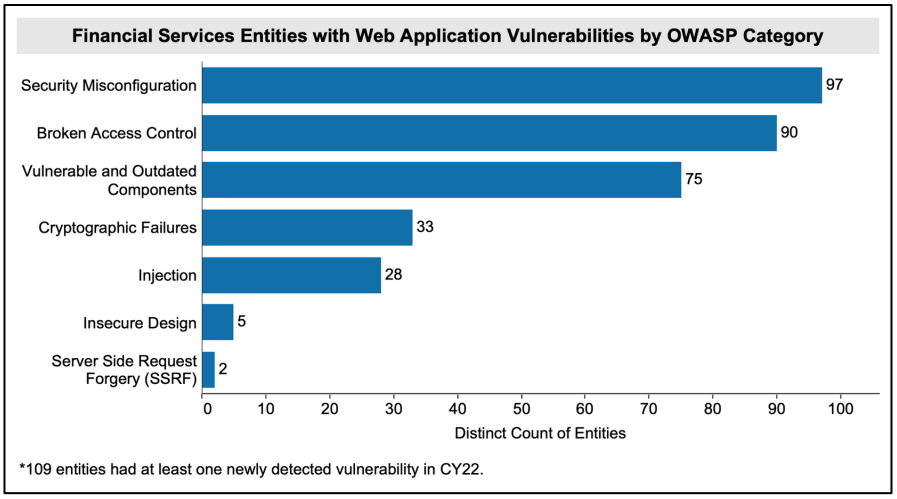


Figure 2: WAS Vulnerabilities Grouped by OWASP Category

At least 85% of scanned entities had web application vulnerabilities that provide threat actors with a variety of opportunities for exploitation that could provide access to sensitive information and an opportunity to affect FS customers' personal data.

- The most prevalent WAS vulnerabilities observed, at 78% of scanned FS entities, were associated with the Security Misconfiguration OWASP category. These vulnerabilities include enabling unnecessary features, using default usernames and passwords, and other improper configurations that facilitate compromise.
- Approximately 70% of scanned FS entities exposed Broken Access Control OWASP category vulnerabilities in their web applications. In 2019, a large FS entity's website failed to properly restrict access to sensitive documents in the websites' backend database, resulting in the public exposure of more than 885 million sensitive documents.[5]
- 66% of scanned FS sector entities exposed vulnerabilities in the Vulnerable and Outdated Components OWASP category. These vulnerabilities allow a threat actor to carry out XXS, SSRF, and buffer overflow attacks by leveraging JavaScript libraries with known vulnerabilities. Exploitation of these vulnerabilities could lead to account takeover and denial of service.
- 21% of scanned FS entities exposed WAS vulnerabilities in the Injection OWASP category, which includes attacks such as XSS and SQL injection. Threat actors capable of leveraging SQL injection could view and modify sensitive information affecting the confidentiality and integrity of customer and stakeholder data.

[5] AJ Dellinger, "Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?" *Forbes,* May 26, 2019, https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean.

Mitigations

- ☐ Maintain a documented list of relevant threats and cyber actor TTPs and ensure proper detection methods. (CPG 3.A *Detecting Relevant Threats and TTPs*)
- ☐ Collect access and security logs, namely (IDS/IDPS), firewall, data loss prevention (DLP), and virtual private network (VPN), and ensure logs are securely stored for a direction informed by risk or pertinent regulatory guidance. (CPG 2.T *Log Collection*, CPG 2.U *Secure Log Storage*)
- ☐ Maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., business email and web browsing). All privileges should be revaluated on a recurring basis to validate continued need for a given set of permissions. (CPG 2.E *Separating User and Privileged Accounts*)
- ☐ Establish and maintain secure configuration baselines for applications and services. (CPG 2.O *Document Device Configurations*)

Poor Encryption Practices Risks Sensitive Data Compromise

The secure transfer of data, often supported through encryption, is an important component of financial transactions and includes web applications and sensitive system to system communications that must occur to validate transactions. Encryption protocols also ensure that a legitimate source sent the data being sent and received. Across scanned and assessed FS sector entities, CISA observed protocols and policies that could allow malicious actors to exploit encryption weaknesses and negatively impact operations.

- CISA observed that 8% of scanned FS entities with "SSL versions 2 and 3 protocol detected" weaknesses. SSL is a deprecated encryption protocol; these versions of SSL have been deprecated since 2011 and 2015 respectively. SSL should not be used on FS entity systems due to the risk that threat actors could carry out machine-in-the-middle attacks (MitM) that allow them to steal sensitive information such as login credentials and banking information.
- CISA observed that 72% of scanned FS entities with "TLS version 1.0 protocol detection" and "TLS version 1.1 protocol deprecated" weaknesses on their systems. These versions of TLS have been deprecated since March 2021 and can also allow a threat actor to perform MitM attacks.
- CISA observed that over half of assessed entities had exposed web applications with insecure transport protocols, including lack of enforcement of the HTTPS secure web transport protocol and HTTP strict transport security (HSTS). Insecure transport protocols are vulnerable to downgrade attacks that can be used to redirect users to malicious domains or servers to compromise user data and session cookies.

Downgrade Attacks: A cyber attack in which a threat actor forces a computer system or protocol to a less secure standard. This is typically used to intercept encrypted traffic. One example is redirecting a user from HTTPS to HTTP.

(MiTM): A cyber attack in which a threat actor exploits weak web-based protocols and relays or alters communications between two parties to make it appear as if a normal exchange is taking place. Threat actors can use this method to gain a foothold during initial access or to obtain sensitive data.

- Multiple assessed entities used weak ciphers and had encryption certificate issues (self-signed and expired). In addition, 25% of scanned entities had weak encryption algorithms associated with Secure Shell (SSH), which is a network protocol used to communicate or transfer data between two computers. These vulnerabilities could result in data disclosures, loss of sensitive information, or MitM attacks.[6]

An expired encryption certificate enabled the breach of a large FS entity in 2017 to go undetected for months, resulting in the compromise of at least 145.5 million individuals' personal information.[7] Maintaining properly configured and updated encryption protocols and policies protects entities' sensitive data.

Mitigations

- ☐ Update all outdated or weak encryption and maintain properly configured and up to date transport layer security (TLS) and encryption protocols. (CPG 2.K *Strong and Agile Encryption*)
- ☐ Establish and maintain secure configuration baselines for applications and services. (CPG 2.O *Document Device Configurations*)

[6] "SSH Server CBC Mode Ciphers Enabled" Tenable, https://www.tenable.com/plugins/nessus/70658, Accessed: March 30, 2023.
[7] GAO, "Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach," August 2018, https://www.gao.gov/assets/gao-18-559.pdf.

Use of Unsupported Software and Windows OS Elevate Entity Risk Profile

CISA scan data showed 168 FS entities exposed outdated software associated with the following vendors: Apache, Atlassian, Bitvise, JQuery, ManageEngine, Microsoft, OpenSSL, PHP, Pulse, SSL/TLS, Tenable, Unix, and Nginx; and at least 10% exposed unsupported versions of Windows OS. Figure 3 presents a graph of the percentage of FS entities running unsupported versions of Windows OS. Exposing outdated versions of software or unsupported OS provides opportunities for threat actors to seek to exploit known vulnerabilities. It is very likely that exposure of unsupported Windows OS increases threat actor targeting and may pose risks of ransomware compromise, according to industry reporting.[8]

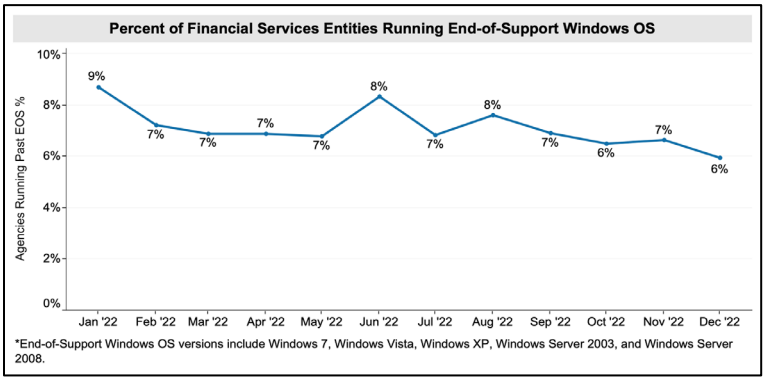


Figure 3: Unsupported Windows Operating Systems

When vendors no longer provide support for an OS, threat actors can exploit both known and disclosed vulnerabilities in addition to developing new zero-day attacks. Since these systems are no longer the focus of security updates and patches, new zero-day vulnerabilites may remain undiscovered for longer periods of time, leaving the systems more susceptible to attacks. CISA encourages FS entities to reduce use and phase out all unsupported OS versions within entity and vendor constraints and stay informed of end-of-support notifications.*

***** End of support Windows OS versions include Windows 7, Windows Vista, Windows XP, Windows Server 2003, and Windows Server 2008. **Of Note:** Windows 8.1 reached end of service on January 10, 2023. CISA expects these numbers to increase due to the recent end of support of Windows 8.1.

Mitigations

- ☐ Develop and maintain comprehensive documentation of assets—tracking current version information to maintain awareness of outdated and unsupported software. (CPG 1.A *Asset Inventory*)

[8] Joel Alcon, "5 Risks of Outdated Software & Operating Systems," *Bitsight,* August 14, 2017, https://www.bitsight.com/blog/outdated-software-issues.

Vulnerable Service Exposure Increases Risk of Initial Access

CISA scans detected internet-accessible vulnerable services (displayed in Figure 4) in 36 distinct FS sector stakeholders (MITRE T1190). These vulnerable services increase the risk of sensitive data compromise and provide initial access vectors to threat actors. Vulnerable services should not be internet-accessible unless there is a valid business use case, and only with the implementation of appropriate compensating controls.

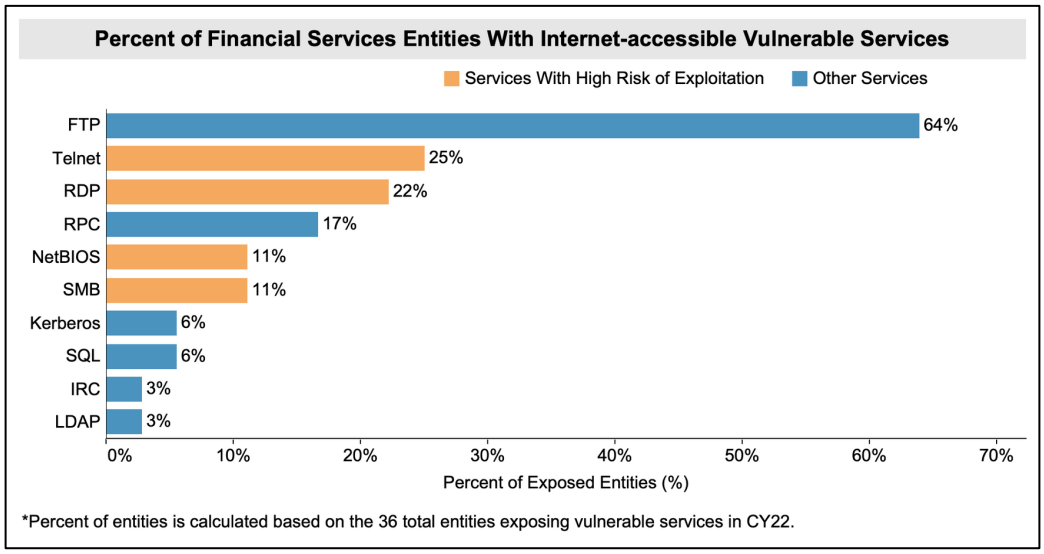


Figure 4: Vulnerable Services

- File transfer protocol (FTP), a file sharing service, is the most prevalent vulnerable service among FS entities and, if misconfigured, can transmit cleartext data susceptible to password sniffing and eavesdropping.
- Remote access services, such as remote desktop protocol (RDP) (MITRE T1210) and Telnet, are the most prevalent "higher risk" services among FS entities that threat actors can use to gain initial access, distribute ransomware, provide vectors for command and control, and exfiltrate data.[9]

[9] CISA, "#StopRansomware: LockBit 3.0," March 16, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a.

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 2.W *No Exploitable Services on the Internet*)
- ☐ Implement network segmentation to isolate critical systems from the corporate network. (CPG 2.F *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 2.U *Secure Log Storage*)

Device Exposure Poses Risk to Physical and IT System Security

CISA observed exposure of assets that, absent compensating or mitigating controls, put scanned FS entities corporate and IT networks at risk. This includes exposure of potential OT devices and unauthorized devices that CISA knows threat actors to target for initial access and to affect operations. In addition, CISA observed other devices that should not be directly accessible to the public internet, such as energy monitoring systems, printers, video conferencing, and camara/monitoring systems. These devices present both IT system concerns and physical security concerns.

- CISA scanning identified at least five FS entities that likely exposed a programmable logic controller (PLC). PLCs are OT devices that are typically utilized for automation of mission critical functions. While there were no associated CVEs with the specific devices, OT systems exposed to the internet pose a significant risk to an entities' network and critical network components. Threat actors are known to target these systems and almost certainly scan for exposure of PLCs, based on industry reporting. Without properly configuring and segmenting OT assets, threat actors have increased opportunities to compromise these assets directly, conduct reconnaissance on FS networks, gain entry into the IT network, or cause larger affects to OT and IT operations.
- CISA VS also observed the probable exposure of unmanaged devices. The detected devices are probably unmanaged because they may not have clear operational need to be connected to entity networks—e.g., Amazon Kindle(s), Nintendo Wii(s), Xbox, PlayStation 3, Slingbox Tuners and TVs, and Blu-ray player(s).

While some systems are designed to be remotely accessible, such exposures increase an entity's overall attack surface and create unnecessary opportunities for threat actors. These unmanaged devices are likely not subject to the same cybersecurity

requirements as authorized assets and, in general, entertainment/personal assets pose unnecessary attack surface exposure.

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 another intermediary). (CPG 2.X *Limit OT Connections to Public Internet*)
- ☐ Implement network segmentation to isolate critical systems, namely OT devices, from the corporate network. (CPG 2.F *Network Segmentation*)
- ☐ Develop and maintain comprehensive documentation of assets to maintain awareness of unmanaged devices. (CPG 1.A *Asset Inventory*)
- ☐ Strengthen account security to include updated encryption protocols, strong passwords, unique credentials, phishing-resistant multifactor authentication (MFA), and the separation of user and privileged accounts. (CPG 2.K *Strong and Agile Encryption*, CPG 2.A *Changing Default Passwords*, CPG 2.B *Minimum Password Strength*, CPG 2.C *Unique Credentials*, CPG 2.H *Phishing-Resistant Multifactor Authentication (MFA)*, and CPG 2.E *Separating User and Privileged Accounts*)

Phishing Weaknesses Increase Threat Actors Probability of System Access

Phishing (MITRE T1566) uses social engineering to either solicit sensitive information through email from targeted users (i.e., user's credentials) or 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. According to open-source research, phishing remained a technique favored by threat actors for initial access in 2022.[10]

- CISA's phishing assessments of FS sector entities revealed that the top two payloads with the greatest user interaction had subject lines referring to company-specific information or user account notifications.
- CISA assessments conducted testing on FS sector participants and despite the security measures in place, 60% of malicious payloads were able to bypass the protective barriers at the network's edge, and 10% of payloads were able to bypass the measures in place to stop them from reaching their target inboxes on individual machines.

[10] "2022 Data Breach Investigations Report," Verizon, last accessed March 14, 2023, https://www.verizon.com/business/resources/reports/dbir/.

- CISA assessments observed that multiple payload types (e.g., embedded word documents and spreadsheets) were delivered and opened via phishing emails. This is in line with open-source reporting identifying HTML and windows document (doc) files as the most prevalent phishing payloads.[11]

Failure to block phishing payloads can result in negative outcomes, including disclosure of information for use in follow-on malicious actions or delivery of malware/ransomware resulting in complete network compromise.[12]

Mitigations

- ☐ Implement phishing-resistant MFA such as FIDO/Web Authentication (WebAuthn) application programming interface (API). (CPG 2.H *Phishing-Resistant Multifactor Authentication (MFA)*)
- ☐ 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 2.M *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 2.I *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.N *Disable Macros by Default*)

VULNERABILITY MANAGEMENT TRENDS

Prolonged Vulnerability Exposures

Prolonged vulnerability exposures increase the opportunity for threat actors to identify weaknesses and develop exploitation strategies and capabilities. Analysis of CISA's data indicates that scanned FS sector entities' responsiveness to address known vulnerabilities and exposures lagged behind CISA's recommended goals for federal agencies. Although FS sector entities are not required to comply with federal agency standards, swift remediation or mitigation activities reduce the risk of compromise. Considerable improvement can be made to reduce vulnerability exposure.

[11] ESET, "Threat Report T2 2022," We Live Security, 2022, https://www.welivesecurity.com/wp-content/uploads/2022/10/eset_threat_report_t22022.pdf.
[12] Checkpoint Research, "Dangeroussavanna: Two-Year Long Campaign Targets Financial Institutions In French -Speaking Africa," https://research.checkpoint.com/2022/dangeroussavanna-two-year-long-campaign-targets-financial-institutions-in-french-speaking-africa/, Accessed: March 31, 2023.

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

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

At the end of CY22, three distinct stakeholders continued to expose KEVs, which is a decrease from the 11 stakeholders who were unable to remediate KEV exposures prior to the end of CY21. However, scanned FS sector entity exposure of critical and high severity vulnerabilities increased from 11% in CY21 to 36% in CY22.

- 85% of KEVs took more than 30 days to remediate, indicating most KEVs were remediated outside CISA's recommended timeframes. While CISA provides specific remediation guidance per new KEV added to CISA's KEV catalog, remediation guidance is typically less than 30 days.
    - KEVs remaining active at the end of CY22 were open for a median of 514 days, an increase from 184 days at the end of CY21. 12% of FS sector entities that exposed KEVs were not able to remediate them prior to the end of CY22.
    - One KEV associated with a CISCO vulnerability, CVE-2020-3452, remained unpatched for a median of 441 days prior to remediation before the end of CY22. 30% of FS sector entities that exposed KEVs exposed this vulnerability prior to its remediation within CY22.
    - Apache Tomcat KEV CVE-2020-1938 and Cisco KEV CVE-2020-3580 remained active at the end of the calendar year and persisted for 690 and 243 median days respectively. Exposure of these KEVs for extended periods increased opportunities for threat actors to exploit these vulnerabilities.

- Remediation of most critical and high severity vulnerabilities by scanned FS sector entities lagged behind CISA's recommended timeframes, with 91% of critical severity vulnerabilities remediated in more than 15 days and 77% of high severity vulnerabilities remediated in more than 30 days (see Figure 5). Critical and high severity vulnerabilities were exposed for a median of 493.1 days active at the end of CY22 compared to 506.4 median days for CY21.

CY22 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	11%	4%	9%	76%
Critical	9%	14%	32%	45%
High	23%	5%	8%	64%
Medium	27%	12%	12%	49%
Low	15%	8%	15%	62%
Grand Total	24%	10%	13%	53%

*Population actively scanned in CY22 includes 308 entities and 5,925 hosts. KEVs are excluded from remediation percentages by severity.

Figure 5: Remediation Timeliness on FS Networks

Remediation of Vulnerability Backlog

Scanned FS sector entities made strides in remediating vulnerabilities on their networks, with an average reduction of 9.5% for CY22 (see Figure 6). This is an improvement from CY21, which saw an average reduction of 5.1%. In CY22 there was significant remediation from May to June, at 37.9%. This sharp decrease was due to a significant reduction in instances of multiple Apache vulnerabilities, including CVE-2021-40438, which led to an 81% reduction of all open KEVs.

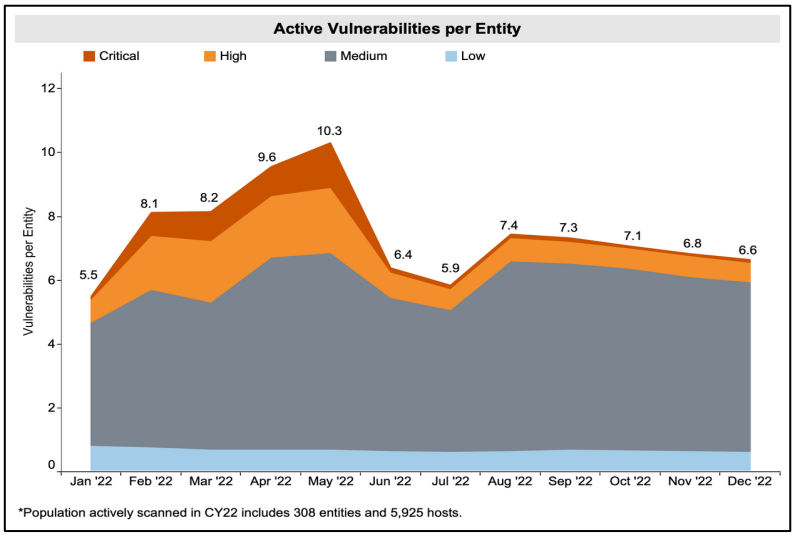


Figure 6: Active Vulnerabilities Per Entity

Sector Enrollment Trends

FS sector enrollment in CyHy VS scanning increased in CY22 by an average of 14 entities per month (See Figure 7). FS entities enrolled in CISA's CyHy VS service during CY22 decreased vulnerability exposure by an average of 20.1% within the first three months of conducting vulnerability scanning. FS sector entities made progress in remediating their backlog of vulnerabilities in CY22.

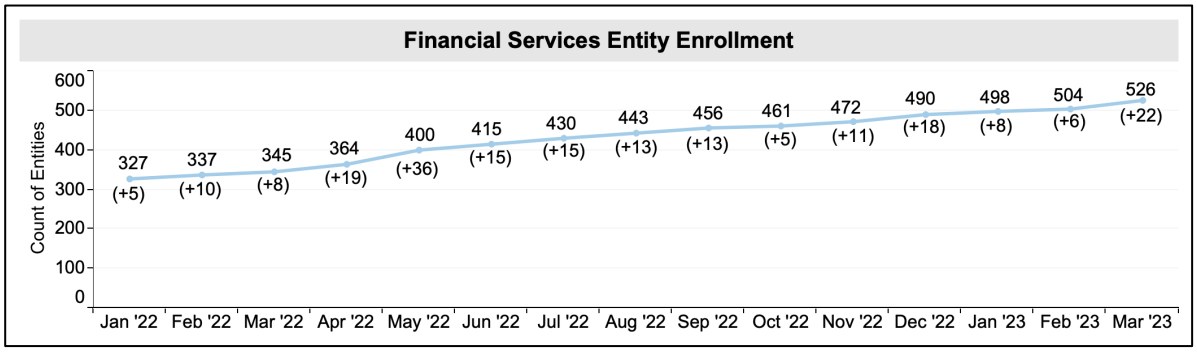


Figure 7: Financial Services Entity Enrollment

CONCLUSION

FS entities can reduce their cybersecurity risk by following the mitigations and recommendations mapped to CISA's CPGs and shared througout this document. For more support, CISA encourages FS sector entities to continue to sign up for free CISA services, such as CyHy VS and WAS. FS 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

This report analyzed data from the following CISA services*:*

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 0–10.*[13] *Nessus references the National Vulnerability Database (NVD) for its vulnerability information.*[14] *The NVD provides CVSS v2 base scores and corresponding severity levels for all 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 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 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. During CY22 FS sector entities participated in the following assessments:*

- ***Remote Penetration Tests (RPTs)*** *simulate the tactics and techniques real world threat actors use 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.*

[13] "Common Vulnerability Scoring System SIG," Forum of Incident Response and Security Teams (FIRST), accessed March 15, 2023, https://www.first.org/cvss.
[14] "National Vulnerability Database," National Institute of Standards and Technology (NIST), accessed March 15, 2023, https://nvd.nist.gov.