VULNERABILITY SNAPSHOT FINANCIAL SERVICES SECTOR (FSS) SEPTEMBER 2023

SCOPE NOTE

This Vulnerability Snapshot is based on analysis of the Cybersecurity and Infrastructure Agency's (CISA) observations of internet accessible information technology (IT) assets from 537 FSS entities (of 645 enrolled) participating in the CISA Cyber Hygiene-Vulnerability Scanning (CyHy-VS) service, 136 entities enrolled in the CISA Web Application Scanning (WAS) service, and industry data during September 2023.

EXECUTIVE SUMMARY

A recent industry report revealed an updated Android banking trojan called "Xenomorph" is targeting more than 35 financial institutions within the sector. The Xenomorph campaign utilizes phishing web pages designed to lure victims into downloading malicious Android applications on their devices, serving as a method of initial access for the threat actors.[1] Previous iterations of Xenomorph were spotted earlier in 2023 and allowed for threat actors, known as Hadoken Security, to completely seize user devices by using the Automatic Transfer System (ATS) feature. Customers of Chase, Amex, Ally, Citi Mobile, Citizens Bank, Bank of America, and Discover Mobile are thought to be prime targets of the Xenomorph campaign(s).[2]

CISA maintains the authoritative source of known exploited vulnerabilities (KEV). Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework. For more information visit: **cisa.gov/known-exploited-vulnerabilities**

CISA highly recommends FSS organizations consider the risk of cyber campaigns in the context of their exposed vulnerabilities, take a risk-informed approach to vulnerability management, and review CISA's Cross-Sector Cybersecurity Performance Goals (CPGs).

FSS entities should continue to maintain awareness of their internet accessible vulnerabilities and take mitigating actions to reduce risk of compromise. During September 2023, CISA identified:

- Known Exploited Vulnerabilities (KEVs) — vulnerabilities that have been actively exploited to compromise public and private entities — associated with various software vendors on FSS entities' internet accessible networks.
- Configuration weaknesses relating to multiple Open Web Application Security Project® (OWASP) categories, including broken access control and vulnerable/outdated components.
- Internet-accessible file sharing and remote access services running over open ports that cyber threat actors routinely leverage to gain access to targeted networks and steal sensitive information.[3] [4]

For specific vulnerability information, please open the embedded spreadsheet.

[1] "Xenomorph Banking Trojan: A New Variant Targeting 35+ U.S. Financial Institutions," The Hacker News, Xenomorph Banking Trojan: A New Variant Targeting 35+ U.S. Financial Institutions (thehackernews.com), Accessed: October 4th, 2023.
[2] Jai Vijayan, "Xenomorph Android Malware Targets Customers of 30 US Banks," DarkReading, Xenomorph Android Malware Targets Customers of 30 US Banks (darkreading.com), Published: September 25, 2023.
[3] Guru, "Hackers Actively Attack RDP Servers To Deploy Ransomware," Cyber Security News, https://cybersecuritynews.com/rdp-servers-actively-targeted-by-hackers/, Published: December 5, 2022
[4] SpecOps Software, "Lessons Learned from the Windows Remote Desktop Honeypot Report," BleepingComputer, https://www.bleepingcomputer.com/news/security/lessons-learned-from-the-windows-remote-desktop-honeypot-report/, Published: January 25, 2023

This document is marked TLP:AMBER: Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

VULNERABILITIES

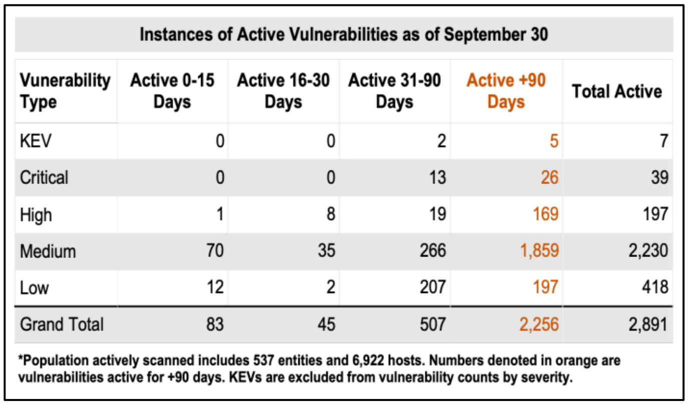
Continued exposure of internet accessible KEVs increases opportunities for compromise.

KEVs are vulnerabilities that have been actively exploited to compromise public and private entities.[5] Among scanned FSS entities, CISA's CyHy-VS identified five distinct active KEVs (Figure 1) associated with the following software developers: Apache, Cisco, PHP, and Sophos. CISA observed that distinct KEVs associated with these vendors persisted from August through September of 2023 across multiple entities within the sector.

September industry scan data remained consistent from August, still showing Microsoft Exchange Server Product(s) vulnerabilities (CVE-2021-27065) that are known to be routinely exploited by People's Republic of China state-sponsored cyber actors (see Figure 1 and attached September vulnerability spreadsheet).[6] [7] Additionally, industry scan data continued to observe instances of Apache's HTTP Server vulnerability that affects version(s) 2.4.48 and earlier that have the "mod_proxy" feature enabled (CVE-2021-40438). This vulnerability allows threat actors to send carefully crafted requests that are subsequently rerouted by the module to an origin server of their choice, allowing for potential access to internal servers.[8] Patches are available for all KEVs, and FSS entities should prioritize remediation of KEVs to reduce the risk of compromise.

Vendor/Software	CVE
Apache	CVE-2021-40438 CVE-2020-1938
Cisco	CVE-2020-3580 CVE-2020-3452
Microsoft	CVE-2021-27065
PHP	CVE-2019-11043
Sophos	CVE-2022-1040

Figure 1: Distinct Active KEVs, September 2023



Instances of Active Vulnerabilities as of September 30

Vunerability Type	Active 0-15 Days	Active 16-30 Days	Active 31-90 Days	Active +90 Days	Total Active
KEV	0	0	2	5	7
Critical	0	0	13	26	39
High	1	8	19	169	197
Medium	70	35	266	1,859	2,230
Low	12	2	207	197	418
Grand Total	83	45	507	2,256	2,891

*Population actively scanned includes 537 entities and 6,922 hosts. Numbers denoted in orange are vulnerabilities active for +90 days. KEVs are excluded from vulnerability counts by severity.

Figure 2: Active Vulnerabilities on FSS Networks from CISA Data

Most identified vulnerabilities persist, increasing risk of compromise.

Vulnerabilities active at the end of September 2023 persisted on entity networks for a median of 298 days, an increase from 256 days in August 2023, based on analysis of CISA's CyHy-VS data. Timely remediation of vulnerabilities can decrease a cyber threat actor's opportunity to exploit them. CISA recommends remediating critical vulnerabilities within 15 days and high vulnerabilities within 30 days. Overall, total instances of active vulnerabilities decreased by about 50 from August to September.

Configuration weaknesses can enable compromise of FSS entities.

CISA's CyHy-VS data showed the scanned FSS entities had various web application encryption vulnerabilities that provide cyber threat actors opportunities to obtain leaked credentials. FSS entities continued to use insecure versions of Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Shell (SSH) encryption on internet-accessible assets, such as web applications and email services. FSS entities exposing vulnerabilities relating to deprecated versions of TLS and SSL increased from 32% in August to 49% in September. This percentage increase may be influenced by the number of entities actively scanned within the period of analysis. CISA data also showed instances of FSS entities exposing the POODLE vulnerability. If successfully exploited, threat actors can deploy man-in-the-middle attacks that facilitate connections to SSLv3 for a protocol downgrade.[9] FSS entities should continue working towards eliminating all instances of deprecated encryption protocol usage to minimize their attack surface and better safeguard their networks.

[5] CISA, "Reducing the Significant Risk of Known Exploited Vulnerabilities," https://www.cisa.gov/known-exploited-vulnerabilities, Accessed: July 7, 2023

[6] See embedded spreadsheet for a detailed list of detected KEVs from CISA and industry scan data.

[7] CISA, "Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors," Alert AA22-279A, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-279a, Accessed: July 7, 2023

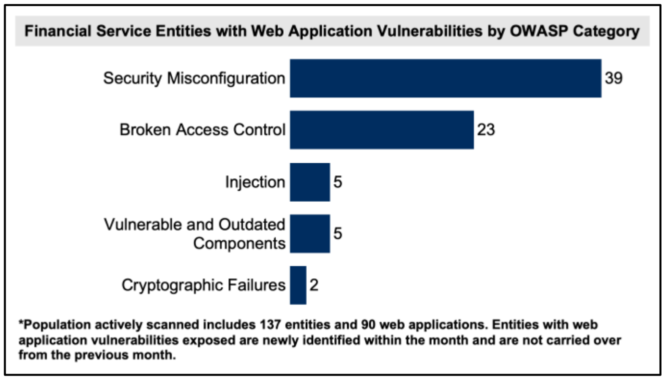
[8] Eduard Kovacs, "Recently Patched Apache HTTP Server Vulnerability Exploited in Attacks," Security Week, Recently Patched Apache HTTP Server Vulnerability Exploited in Attacks - SecurityWeek, Published: November 29, 2021.

[9] Michael Cobb, "The POODLE vulnerability and its effect on SSL/TLS security," Tech Target, The POODLE vulnerability and its effect on SSL/TLS security | TechTarget, Accessed: October 4, 2021.

Web application weaknesses known to be targeted by cyber threat actors.

During September 2023, the most observed web application vulnerabilities were in the security misconfiguration OWASP category. Security misconfigurations enable end-users to be more susceptible to sniffing and clickjacking attacks. According to industry reporting, security misconfigurations are the most common exploitable perimeter exposure used by ethical hackers and cyber threat actors, followed closely by exposed web services and vulnerable software.[10]

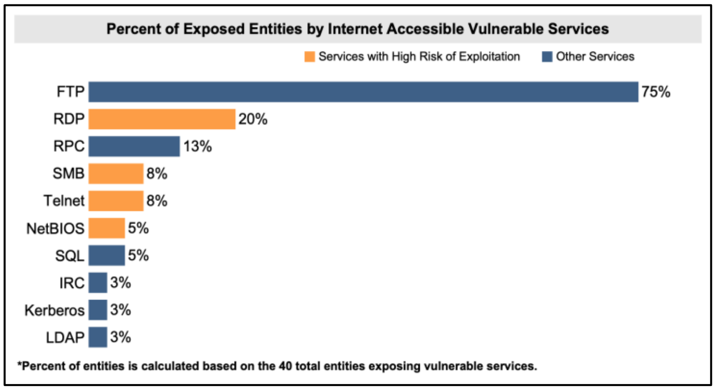
The second most observed web application vulnerabilities were in the broken access control OWASP category. Path-based vulnerabilities are the most exploited broken access control vulnerabilities by cyber threat actors targeting the FSS.[11] When internal object references, such as a sensitive file or database records are exposed by an application, cyber threat actors may exploit this vulnerability to compromise the confidentiality of sensitive customer and business data.[12]



*Population actively scanned includes 137 entities and 90 web applications. Entities with web application vulnerabilities exposed are newly identified within the month and are not carried over from the previous month.

Figure 3: WAS Vulnerabilities Grouped by OWASP Category

WAS scanning also showed FSS entities with web application vulnerabilities in the cryptographic failures OWASP category. In OWASP's 2023 rankings list, the cryptographic failure category currently ranks 2nd in terms of frequency and severity of impact.[13] Missing or improper encryption methods can make sensitive data vulnerable to exploitation while both in transit and at rest.[14]



*Percent of entities is calculated based on the 40 total entities exposing vulnerable services.

Figure 4: Vulnerable Services from CISA Data

Some FSS entities continued to use internet accessible, vulnerable services.

CISA and industry data identified that file transfer protocol (FTP), remote desktop protocol (RDP), and SQL services accounted for just under half of the vulnerable services detected on internet accessible FSS entity networks, remaining consistent from the previous month. FTP, a file sharing service, continues to be the most prevalent vulnerable service among FSS entities with no change from the previous month. If misconfigured, FTP can transmit cleartext data susceptible to password sniffing and eavesdropping.[15]

SQL services were exposed by 5% of scanned FSS entities, also remaining consistent with the month of August. Exposed SQL services are a popular target for threat actors who leverage them to deploy ransomware.[16] Also observed were additional vulnerable services that are a high risk of exploitation for initial access, such as Telnet, Network Basic Input/Output System (NetBIOS), and Server Message Block (SMB).[17] Vulnerable services should not be internet

[10] Bishop Fox Team, "2022 SANS Survey Report," Key Findings, SANS Report: Inside the Minds & Methods of Modern... | Bishop Fox, Accessed: July 7, 2023
[11] Tom Kellermann, "Top 10 Application attack trends in financial sector | Cyber Security in Financial Services | *Contrast Security*," Security Boulevard, https://securityboulevard.com/2022/12/top-10-application-attack-trends-in-financial-sector-cyber-security-in-financial-services-contrast-security/, Published: December 5, 2022
[12] Mihaela Marian, "What Is Broken Access Control and How to Keep Your Organization Safe?," *Heimdal,* What Is Broken Access Control and How to Keep Your Organization Safe? (heimdalsecurity.com), Accessed: July 7, 2023
[13] Vamona D'Souza, "OWASP Top 10 Vulnerabilities 2023," Edu Dwar, published July 7, 2023 OWASP Top 10 Vulnerabilities 2023 - Edudwar
[14] Sudip Sengupta, "OWASP Top 10 Cryptographic Failures A02 – Explained," Crashtest Security, Cryptographic Failures Vulnerability - Examples & Prevention (crashtest-security.com), Published: June 7, 2022
[15] Jessica Groopman, "7 common file sharing security risks," *TechTarget*, https://www.techtarget.com/searchcontentmanagement/tip/7-common-file-sharing-security-risks, Published: September 21, 2022
[16] SC Staff, "Novel FreeWorld ransomware deployed in attacks against Microsoft SQL servers," SC MEDIA, https://www.scmagazine.com/brief/novel-freeworld-ransomware-deployed-in-attacks-against-microsoft-sql-servers, Published: September 5, 2023
[17] CISA, "Cybersecurity Advisory AA22-137A," Weak Security Controls and Practices Routinely Exploited for Initial Access | CISA, Accessed: July 7, 2023

accessible without a valid business use case, and the entity implements appropriate compensating controls.

FSS entities using unsupported versions of software pose an increased security risk.

Analysis of CISA data identified FSS entities exposing vulnerabilities associated with outdated web server software, specifically version(s) of Apache, Apache Tomcat, Nginx, and OpenSSL, which increase cybersecurity risks. If successfully exploited, these vulnerabilities could enable cyber threat actors to conduct a variety of attacks against those applications or services, such as denial-of-service (DoS), Buffer Overflow, and Remote Code Execution (RCE) attacks. To reduce the risk of compromise, CISA recommends outdated software be replaced with supported versions.

Increased email security could lower potential for phishing attacks.

Industry scan data revealed that at least 1,412 FSS entities had insecure DomainKeys Identified Mail (DKIM) configurations due to missing or malformed DKIM authentication records; a decrease from 1,575 entities in August. DKIM being implemented allows a domain to "watermark" their emails to protect against email spoofing, making spam and phishing emails easier to identify.[18] Additionally, leveraging the Domain Based Message Authentication Reporting (DMARC) security authentication protocol also helps verify email senders in conjunction with DKIM. DMARC allows for further authentication acceptance and generates a report each time a message fails authentication.[19]

SECTOR ENROLLMENT TRENDS

FSS enrollment in CyHy-VS scanning increased in September 2023 by 23 entities.

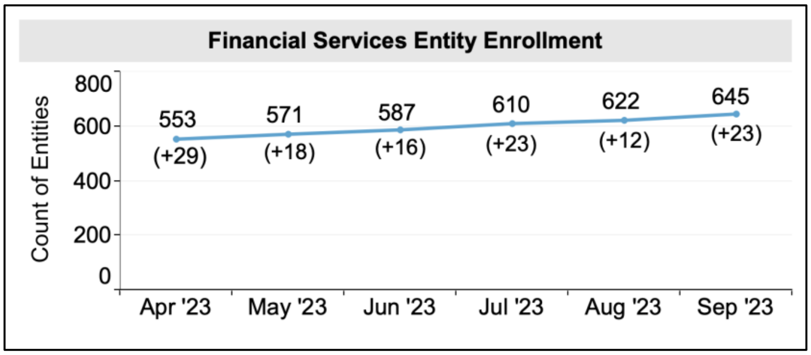


Figure 6: FSS CyHy-VS Total Enrollment

[18] CISA, "Resource Materials," CISA INSIGHTS: Enhance E-mail and Web Security | CISA, Accessed: July 7, 2023
[19] "DKIM vs. DMARC," EASYDMARC, DKIM vs. DMARC | EasyDMARC, Published: November 83, 2022.

OPPORTUNITIES FOR ACTION

Near Term

- Prioritize remediation of vulnerabilities using a risk-based approach and implement patches as they become available to reduce exposure windows.
  - For vulnerabilities with no available patches, FSS entities should implement compensating controls to reduce the risk of compromise and review remediation processes to reduce exposure windows.
  - Consider leveraging CISA's SSVC calculator to assist with prioritizing known vulnerabilities.[20]
- CISA recommends FSS entities remediate all KEV exposures.
  - Entities are encouraged to closely monitor the KEV catalog for new additions and remediate them within CISA's recommended guidelines.
  - Entities should also closely monitor their systems for any indicators of compromise (IOCs) that may have occurred while KEVs were exposed.
- Identify and monitor internet of things (IoT) and industrial internet of things (IIoT) devices and get Stuff Off Search (S.O.S.) to reduce internet attack surfaces.
- Remain aware of the latest advisories and resources CISA provides in response to recent geopolitical events, threat activity, and other emerging vulnerabilities. Click here to subscribe.
- Enroll or continue participation in CISA's no-cost CyHy-VS and other services to maintain awareness of vulnerabilities and inform actions to reduce risk of compromise.
  - **Note:** Cyber threat actors are motivated to leverage the vulnerabilities identified in this summary to disrupt national critical functions and target FSS entities for financial or politically motivated crimes. CISA encourages the FSS to email vulnerability@cisa.dhs.gov to enroll in CyHy-VS or other services.

Longer Term

- Use CISA's CPGs to create a baseline of cybersecurity practices.
  - CISA's CPGs are a prioritized subset of IT and OT cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. They are intended to help small- and medium-sized organizations kickstart their cybersecurity efforts.
- Monitor end-of-support notifications and update or replace unsupported OSs.
  - If unable to update or replace, implement network segmentation of the unsupported OSs to isolate vulnerable systems. This reduces potential impacts of compromise.
- Use best practices for identity and access management (IAM) by implementing phishing-resistant multifactor authentication (MFA), using strong passwords, and limiting user access through the principle of least privilege.
- Use the OWASP Top Ten list and implement web application firewalls (WAFs) to reduce vulnerabilities on web applications.

[20] CISA, "SSVC," Stakeholder-Specific Vulnerability Categorization | CISA, Accessed: July 7, 2023