FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 13 October 2025 | Issue 304

This report elevates this week's top risks to assist community institution information security and technology teams in proactively protecting their financial institution from dangers that can impair its ability to operate and avoid compliance, economic, legal, regulatory, and reputational impact.

This Week's Threats

Fraud Campaigns

- Business Email Compromise
- Customer Impersonation (Call Center)
- Man-in-the-Middle Malvertizing

System Vulnerabilities

Adobe, Amazon (Multiple), Azure, BeyondTrust (Secrets Mgmt.), Broadcom, Cisco, Cygwin, Dell, Debian, Delta Electronics, MULTIPLE F5 (BIG-IP), Fortinet, FSOS, Faith Rucker uses ShareFile to share documents securely with you - Redacted, Google, Grafana, Hitachi, HP, HPE, IBM, IGEL OS, Juniper, Lenovo, Linux, Microsoft (Multiple), Mozilla, NVIDIA, Oracle, Powershell, Red Hat, Rockwell Automation, SAP, Schneider Electric, Siemens, Ubuntu, VMware, Wireshark, and z/OS.

Themed Phishing and Smishing Campaigns

Please see the Phishing Daily Digest for all activities. Use keywords for AV blacklists.

Subject Keywords: 1st New Home, Adult Dating, Amazon, Christopher M. Gorman, Court Summons, Dropbox, Expense Report Google Docs, Fake Invoice, Fraud Withdrawal, KJS Inquiry, New Order, New Submission From, Notary, Peer_Review_Pcm-incDOC, Pending Signature, PPP Loan, Rapid7, Settlement Agreement, SKYSEA, Temporarily Disabled, Urgent, and Zoom.

Threats, Malware, Cyber Campaigns, and Adversaries

- AdaptixC2
- Amatera Stealer
- Astaroth
- Agent Tesla
- AsyncRAT
- Aura Stealer
- BeaverTail
- BitStep RAT
- CHILLYHELL
- Dark Crystal
- GolangGhost
- GULoader
- HardHat RAT
- ICEBITE.PYTHON
- KeyPlug
- LummaStealer
- MultiRat
- Netsupport RAT
- Nitrogen Loader
- NotDoor
- Oyster
- Rhadamanthys Stealer
- Remcos
- SHADOWPAD
- SocGholish
- SocksShell
- SparkRAT
- SquidLoader
- Vanguard Stealer
- VMScape

- KongTuke Malware
- LAMEHUG
- Latrodectus
- Xloader
- Xworm
- ZynorRAT

NEWS AND RISK INFORMATION

All SonicWall Cloud Backup users had firewall configurations stolen. “Threat actors accessed firewall configuration backup files, potentially exposing encrypted credentials and configuration data … SonicWall has published a list of impacted devices to the MySonicWall portal, and customers can access it by navigating to Product Management > Issue List.” (Security Week)

Chinese hackers abuse geo-mapping tool for year-long persistence. ”Chinese APT group Flax Typhoon exploited ArcGIS Server's Server Object Extension (SOE) to maintain undetected access in a target network for over a year. The attackers used valid admin credentials to deploy a malicious Java SOE.” (Bleeping Computer)

FBI takes down BreachForums site used to extort Salesforce customers. “On 9 October, the FBI reportedly completed a takedown of a BreachForums domain used by ShinyHunters as a data leak extortion site for the recent wave of attacks on Salesforce customers.” (SC World)

New Rust-based malware "ChaosBot" uses Discord channels to control victims' PCs. “Cybersecurity researchers have disclosed details of a new Rust-based backdoor called ChaosBot that can allow operators to conduct reconnaissance and execute arbitrary commands on compromised hosts.” (Hacker News)

Researchers warn of widespread RDP attacks by a 100K-node botnet. “A coordinated botnet campaign involving over 100,000 IP addresses from more than 100 countries has been targeting Microsoft Remote Desktop Protocol (RDP) services in the United States. The campaign began on October 8, 2025.” (Security Affairs)

RondoDox botnet targets 56 n-day flaws in worldwide attacks. “A new large-scale botnet called RondoDox is targeting 56 vulnerabilities in more than 30 distinct devices, including flaws first disclosed during Pwn2Own hacking competitions. The attacker focuses on a wide range of exposed devices, including DVRs, NVRs, CCTV systems, and web servers and have been active since June.” (Bleeping Computer)

Seventy-seven percent of employees leak data via ChatGPT, report finds. “Eighteen percent of enterprise employees paste data into generative AI tools, and over 50% of those pastes include corporate information. Notably, 77% of online LLM access is to ChatGPT, with 43% of enterprise users engaging with ChatGPT alone.” (sSecurity Planet)

VMware security advisory. “VMware released a security advisory addressing critical vulnerabilities in VMware Tanzu for MySQL on Kubernetes. These bugs affect versions prior to 2.0.0. The vulnerabilities could expose organizations to significant security risk.” (Canadian Centre for Cybersecurity)

THREAT OF THE WEEK

F5 cyber incident and SAP vulnerability highlight this week’s risks.

F5 Products Victimized in a Cyber Incident

Summary

On October 15, technology firm F5 announced that a sophisticated nation-state threat actor accessed and downloaded files from the firm’s systems. The exfiltrated files included source code and undisclosed vulnerability information for the widely used F5 BIG-IP platform. The threat actor’s access to F5’s proprietary source code could provide a technical advantage in exploiting F5 devices and software.

FS-ISAC immediately established a Spotlight Flash call to share additional information for members. Additionally, a dedicated Connect channel has been established for members to obtain current news and information regarding the incident.

Remediation

Institutions using impacted products should:

- **Update to the latest versions.** Updates are available for BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM, and should be installed as soon as possible. Vulnerability information and related updates are available in the F5 Quarterly Security Notification (October 2025).
- **Inventory impacted devices.** Identify BIG-IP hardware devices and instances of BIG-IP F5OS, BIG-IP TMOS, Virtual Edition (VE), BIG-IP Next, BIG-IQ software, and BNK/CNF. Note whether devices and instances are accessible from the public internet and whether they are end-of-support. Public-facing and end-of-support systems are at greater risk and should be addressed with the greatest urgency.
- **Harden or decommission impacted devices.** Please see the Cybersecurity Infrastructure and Security Agency (CISA) guidance on mitigating the risk from internet-exposed management interfaces and F5 guidance on hardening F5 systems. Network defenders are strongly encouraged to disconnect and decommission any F5 systems past the end of support.

Additional Resources

Please see the following resources for more information:

F5 Resources
- K000154696 - F5 Security Incident
- F5 SEC 8-K Filing
- F5 SEC 8-K Filing Exhibit 99.1 - Disclosure Statement
- Quarterly Security Notification (October 2025)
- K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system

FS-ISAC Resources
- FS-ISAC Flash Report -15 Oct 2025
- FS-ISAC Rapid Response Call
- Member sharing - F5 Discloses Security Incident

Recommended Resources from CrowdStrike (subscription required)
- Falcon-Sensor-for-F5-BIG-IP-VE-17-1-3-and-17-5-1-3
- Intelligence report - csa-251079
- Intelligence report - csa-250969

Recommended Resource from Mandiant
- Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors

Government Partners Resources
- CISA - ED 26-01: Mitigate Vulnerabilities in F5 Devices
- UK NCSC - Confirmed compromise of F5 network
- CCCS - AL25-014 Security Incident impacting F5

SAP NetWeaver Vulnerability Enables DoS Attacks

Summary

Cyware warns of a “newly disclosed vulnerability (CVE-2025-42902) in SAP NetWeaver AS ABAP and ABAP Platform that allows unauthenticated attackers to crash server processes by sending corrupted

SAP Logon or Assertion Tickets. Rated as Medium severity with a CVSS score of 5.3, the flaw stems from a NULL pointer dereference, causing memory corruption and DoS conditions. SAP has released patches and advisory notes to address the issue.

Remediation

End users should immediately apply updates.

THREAT INTELLIGENCE UPDATE

Oracle E-Business Zero-Day Vulnerability

Summary

On 4 October, Oracle's CTO issued a security advisory about CVE-2025-61882 (9.8 CVSS 3.x), an unauthenticated remote code execution vulnerability. The advisory recommended that customers update Oracle E-Business Suite versions 12.2.14-12.3.3 immediately. Google's Threat Intelligence Group (GTIG) also provided commentary indicating Clop exploited multiple Oracle E-Business vulnerabilities, including CVE-2025-61882, to steal large amounts of data from several victims in August 2025.

Clop is historically known for mass exploitation and extortion campaigns of MOVEit, Fortra GoAnywhere, Cleo, and other managed file transfer (MFT) solutions. On 7 October, CrowdStrike published a blog post assessing with moderate confidence that the actor GRACEFUL SPIDER, the company's name for the Clop cybercriminal group, was involved in a campaign exploiting the recently disclosed Oracle E-Business Suite (EBS) vulnerability (CVE-2025-61882).

The first known exploitation reportedly occurred on 9 August. However, CrowdStrike cautioned that it could not rule out the possibility of multiple actors exploiting the vulnerability. CrowdStrike reiterated that the public availability of a proof-of-concept (PoC) exploit will almost certainly encourage threat actors to weaponize exploits against internet-exposed EBS applications.

FBI Seizes BreachForum Domain

Summary

On 10 October, a recently created domain reviving the cybercrime forum BreachForums was seized by the US Department of Justice, the FBI, and France's BL2C cybercrime unit, with the support of the Paris Prosecutor's Office. The website reappeared as a dedicated extortion portal to publish data stolen from Salesforce customers who refused to pay.

The takedown activity coincides with the deadline set by the Scattered Lapsus$ Hunters group of 10/10/2025 at 11:59 PM EST. Following the takedown, an alleged ShinyHunters statement claimed there was no impact on the Salesforce campaign. At the time of writing, the Scattered Lapsus$ Hunters Tor-based leak site remains operational.

JUST FOR COMMUNITY INSTITUTIONS

NY State Institutions – Are You Compliant?

Summary

On 1 November, the final phase of New York State's Cybersecurity regulation (500) goes into effect. Licensed financial institutions in the state are well familiar with the many regulations, risk management, and technology requirements to protect themselves and their customers.

The final requirements include the following components:

- Enhanced Multi-Factor Authentication (MFA) Requirements (Section 500.12).
- Asset Management (Section 500.13(a)).

REGULATORY AND GOVERNMENT UPDATES

Sector Financial Institution Letter and Other Announcements

FRB:

- Federal Reserve Board announces expanded operating days of two large-value payments services, Fedwire® Funds Service and the National Settlement Service (NSS), to include Sundays and weekday holidays (10 October)

FDIC:

- FIL-48-2025, Frequently Asked Questions Regarding Suspicious Activity Reporting Requirements (10 October)

NCUA:

- Agencies' Issue Frequently Asked Questions on Suspicious Activity Reporting Requirements (9 October)

OCC:

- OCC 2025-31, Fair Housing Act: Update to Fair Housing Lender Posters, (15 October)
- OCC 2025-31, Bank Secrecy Act/Anti-Money Laundering: FinCEN Frequently Asked Questions on Suspicious Activity Reporting (9 October)

RESILIENCE UPDATE

JPMorganChase Launches $1.5 Trillion Security and Resiliency Initiative

Summary

JPMorganChase (Chase) announced on their website, "the Security and Resiliency Initiative, a $1.5 trillion, 10-year plan to facilitate, finance, and invest in industries critical to national economic security and resiliency. As part of this new initiative, JPMorganChase will make direct equity and venture capital investments of up to $10 billion to help select companies primarily in the United States enhance their growth, spur innovation, and accelerate strategic manufacturing."

In addition to other areas, Chase reveals they intend to focus on "Frontier and Strategic Technologies, including AI, cybersecurity, and quantum computing."

Read the entire press release.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- Security Advisory: Software Supply Chain Risk: Protecting Against NPM Software Dependencies
- The Timeline for Post Quantum Cryptographic Migration
- Security Advisory: Protecting CRM and SaaS Platforms

- The Business Information Security Officer: Actionable Advice from Practitioners in Four Industries
- Navigating Cyber 2025
- Define the Role, Limit the Risk: The Roles and Responsibilities of AI Usage in Financial Services
- Cross-Sector Mitigations: Scattered Spider | Guidance for Proactive Defense
- From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector
- Leveling Up: A Cyber Fraud Prevention Framework for Financial Services

See the complete list of Knowledge Resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- FinCyber Today Podcast Season 2
- FinCyber Today Podcast Season 1

UPCOMING EVENTS

Americas

Members can enroll in the Member Services app to attend events.

- 20 October | Monthly CIAC Webinar
- 29 October | CIAC and COFFE Open Forum
- 31 October | Member Success Webinar
- 12 November | Executive Protection Council Meeting

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190