FS-ISAC | Risk Summary Report

Global Cyber Threat Level | Americas: EMEA: APAC:

Week of 10 February 2025 | Issue 269

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 their ability to operate and avoid compliance, economic, legal, regulatory, and reputational impact.

This Week's Threats

Fraud Campaigns

- ACH Fraud
- Account takeover (phone)
- Business Email Compromise
- Smishing transaction alert
- Unauthorized withdrawals
- Wire fraud diversion

System Vulnerabilities

Adobe, Amalogon, Apache, Apple, Aura, Avaya, Check Point, Cisco, Cygwin, Debian, Dell, F5, Fortinet, GitLab, GnuTLS, Hitachi, HP, HPE, IBM, Intel, Ivanti, Juniper, Lenovo, Linux, Microsoft, Nvidia, Oracle, Red Hat, RSA, Samsung, SUSE, Trimble Cityworks, Ubuntu, VMware, and Xerox.

Themed Phishing and Smishing Campaigns

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

Subject Keywords: Amazon, ATT NEEDED 02/10, Beneficiary Dispute, BILL#Ref #64360655, Collaboration on an upcoming project, Collaboration request, DocuSign, Fidelity National Title, Fraudshare, Gift Card, Global Management Partners, Insurance, Outbound Funds, Payment confirmation REF, PayPal, QuickBooks, Review Your Card Account, Timesheet Due Today, and wiring instructions.

Threats, Malware, Cyber Campaigns, and Adversaries

- Astaroth
- AsyncRAT
- BeaverTail (InvisibleFerret)
- Black Basta
- BLACKWIDOW (aka Lotus)
- Bumblebee (aka ShellSting, Shindig)
- CellikRAT V4.0 Malware
- ClickFix/ClearFake
- Credential Pharming
- Grandoreiro
- Latrodectus
- LandUpdate808
- LummaStealer
- MetaStealer
- Mispadu
- Nitrogen
- Payroll Diversion
- SocGholish
- SparkRAT
- Typosquatting
- Umbral Stealer
- Xloader
- Xworm
- Zloader

NEWS AND RISK INFORMATION

Attackers exploit cryptographic keys for malware deployment. “Threat actors are using publicly exposed cryptographic keys - ASP.NET machine keys - to manipulate authentication tokens, decrypt protected information, and insert harmful code into susceptible web servers, creating opportunities for unauthorized control and long-term access.” (Data Breach Today)

Breach roundup: hacker claims 20 million OpenAI logins taken. “The hacker posted a sample of user email addresses and passwords claiming, ‘I have more than 20 million access codes to OpenAI accounts. If you want, you can contact me - this is a treasure’ … OpenAI, which operates the popular ChatGPT generative artificial intelligence platform, has not issued a statement about the breach claim.” (DataBreach Today)

Agents and the future of AI threats. “If agentic AIs arrive in 2025, they won’t just answer questions, they will be able to think and act, transforming AI from an assistant that responds to prompts, into a peer, or even an expert that can plan out tasks, interact with the world, and solve the problems it encounters.” (Malware Bytes)

Ransomware attackers turn to workers for data breach access. “Malware operators are now pitching victims on the prospect of infecting additional machines on their company network. The offer comes as part of the notification pop-up that the standard ransomware infection — in this case a variation of the DoNex malware — would otherwise provide. While users would originally be served with a notification of infection and a ransom demand with payment instructions and links, there is now an additional offer asking the user to do the criminals’ dirty work.” (SC Media)

THREATS OF THE WEEK

Multiple system vulnerabilities highlight this week’s risks.

Apple Zero-Day

Summary

CVE-2025-24200 An authorization issue was addressed with improved state management. This issue is fixed in iPadOS 17.7.5, iOS 18.3.1, and iPadOS 18.3.1. A physical attack may disable USB Restricted Mode on a locked device. Apple is aware of a report that this issue may have been exploited in an extremely sophisticated attack against specific targeted individuals.

The vulnerability affects iPhone XS and later, iPad seventh generation and later, iPad mini fifth generation and later, all iPad Pro 11-inch generations, iPad Pro 13-inch, iPad Pro 12.9-inch third generation and later, and iPad Air third generation and later.

CVE-2023-41064 A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 16.6.1 and iPadOS 16.6.1, macOS Monterey 12.6.9, macOS Ventura 13.5.2, iOS 15.7.9 and iPadOS 15.7.9, macOS Big Sur 11.7.10. Processing a maliciously crafted image may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

CVE-2023-41061 A validation issue was addressed with improved logic. It is fixed in watchOS 9.6.2, iOS 16.6.1, and iPadOS 16.6.1. A maliciously crafted attachment may result in arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Risk

MSSP Alert reports that Apple did not provide additional details regarding the attacks but findings from Citizen Lab suggest the zero-day exploitation is to facilitate commercial spyware compromise. The development comes more than a year after reported attacks involving the BLASTPASS exploit, which combined the Apple zero days CVE-2023-41064 and CVE-2023-41061 to spread NSO Group's Pegasus spyware.

Remediation

Institutions should research applications and iOS for vulnerabilities and patches to reduce risk.

Additional references

- https://support.apple.com/en-us/122173
- https://support.apple.com/en-us/122174

Adobe Arbitrary Code Execution

Summary

Multiple vulnerabilities have been discovered in Adobe products, the most severe of which could allow for arbitrary code execution. There are no reports of active exploitation as of the time of this report.

Institutions should review the complete list of vulnerabilities to determine if their institution is at potential risk and take remedial action.

Related Material

https://helpx.adobe.com/security/Home.html

Fortinet Remote Code Execution

Summary

An incorrect privilege assignment vulnerability [CWE-266] in the FortiOS security fabric may allow an authenticated admin whose access profile has the Security Fabric permission to escalate their privileges to super-admin by connecting the targeted FortiGate to a malicious upstream FortiGate they control. CVE-2024-40591

A stack-based buffer overflow [CWE-121] vulnerability in FortiOS CAPWAP control may allow a remote unauthenticated attacker to execute arbitrary code or commands via crafted UDP packets, provided the attacker can evade FortiOS stack protections and provided the fabric service is running on the exposed interface. CVE-2024-35279

Related Material

- https://www.fortiguard.com/psirt/FG-IR-24-535
- https://www.fortiguard.com/psirt/FG-IR-24-160
- Visit https://www.fortiguard.com/psirt for a complete list of other available patches

Microsoft Patches 63 Vulnerabilities

Summary

Microsoft has released patch information for 63 product vulnerabilities. While the majority of CVEs are classified as “less likely exploitation” there are currently no workarounds or mitigations. Additionally, Microsoft is republishing four non-Microsoft vulnerabilities.

Institutions should review the complete list and develop action plans as necessary.

Related Material

For a complete list of vulnerabilities, click here.

SAP Patches 21 Vulnerabilities

Summary

On 11 February SAP released 19 new security notes and two updates to previously released security notes.

Related Material

For a full list of products, visit SAP.

THREAT INTELLIGENCE UPDATE

Concerns Grow Over Chinese Startup DeepSeek

Growing information about DeepSeek sparks concern.

Summary

Issue 268 of the Risk Summary Report noted two recent warnings regarding DeepSeek.

Since then, several publications have reported that US lawmakers are considering a ban on Chinese startup DeepSeek's AI chatbot on government devices. Lawmakers expressed concern that because DeepSeek stores data in China, the app could provide user information to the Chinese government and is subject to Chinese data-sharing laws.

The DeepSeek app reportedly sends user data to servers controlled by ByteDance, the Chinese company that owns TikTok. The push for a ban comes after South Korea, Australia, and Italy blocked the app on their government-run systems.

DeepSeek made headlines early in 2025 as it claimed its latest AI model has largely the same capabilities as ChatGPT and other leading AI chatbots but requires less computing power. The chatbot was the most downloaded app in the US, and the startup offers its models as open source.

Microsoft and OpenAI are investigating whether a group connected with DeepSeek accessed OpenAI's proprietary data without permission. Last fall, Microsoft's security team reportedly noticed large amounts of data being exfiltrated in the activity they believe may have been linked to DeepSeek.

Risk

The data stolen could have been used to bolster DeepSeek's model, allowing the startup to leapfrog OpenAI's work.

FRAUD UPDATE

New Account Fraud

Summary

FS-ISAC's Fraud Intelligence Community reports new account deposit fraud involving US Treasury checks. The activity is not confined to a specific geographical area.

Remediation

Institutions should notify new account officers about this trend and reinforce Know Your Customer guidelines.

If suspicious activity is detected when an account is opened, instruct new account officers to consult with their manager or fraud department and exercise additional due diligence.

GOVERNMENT AND REGULATORY NEWS

NCUA: Exam Scheduling Policy Changes

Summary

During its December 2024 meeting, the NCUA Board approved changes to the agency's examination scheduling policy for federally insured credit unions (FICUs) as part of approving the 2025–2026 budget. These examination scheduling changes were noted in Letter to Credit Unions 25-CU-01, NCUA's 2025 Supervisory Priorities.

The changes outlined in this letter became effective on 1 January 2025. The changes allow the NCUA to:

- Extend the time between examinations for qualifying credit unions with assets of $1 billion to $10 billion
- Improve coordination with state supervisors for examinations of qualifying large federally insured, state-chartered credit unions (FISCUs)
- Better respond to emerging risks and priorities using available resources

Read the Letter to Credit Unions

NCUA: Federal Credit Union Operating Fee Schedule for 2025

Summary

The NCUA Board unanimously approved the agency's 2025 operating and capital budgets at its December 2024 meeting. As a result of that decision and other factors, federal credit union operating fees will decrease by an average of approximately 1.2% in 2025. Additionally, the operating fee exemption threshold was increased from $2 million to $2.08 million. Federal credit unions with a four-quarter average of $2.08 million or less in total assets are exempt from the operating fee.

Read the Letter to Federal Credit Unions

NCUA: Federal Credit Union Post-Examination Survey

Summary

The NCUA has been using a voluntary post-examination survey for examinations of federal credit unions since 2021. This critical feedback helps the NCUA evaluate our examination processes; credit unions have used open-ended questions to submit numerous useful suggestions.

Read the Letter to Federal Credit Unions

Rodney Hood Appointed Acting Comptroller of the Currency

Summary

On 7 February, former NCUA Chair Rodney E. Hood was appointed acting comptroller of the currency. Hood's appointment is effective 10 February.

PRACTICAL KNOW-HOW FROM YOUR FELLOW MEMBERS

Recent Publications

- More Opportunity, Less Risk: 8 Steps to Protect Financial Services Data with GenAI
- FS-ISAC 2024 Year-in-Review Report
- Stop the Scams: A Phishing Prevention Framework for Financial Services
- Ransomware Essentials: A Guide for Financial Services Firm Defense
- Deepfakes in the Financial Sector: Understanding the Threats, Managing the Risks
- Building Cryptographic Agility in the Financial Sector
- Protecting Financial Data with Encryption Controls
- Principles for Financial Institutions' Security and Resilience in Cloud Service Environments
- Business Information Security Officer (BISO) Program and Role
- Resilience in Action - Lessons from the Field
- Navigating Cyber 2024: Annual Threat Review and Predictions
- Digital Operational Resilience Act (DORA) Implementation Guidance
- Financial Services and AI: Leveraging the Advantages, Managing the Risks
- LockBit: Access, Encryption, Exfiltration, and Mitigation

See the full list of Knowledge Resources

INSIGHTS FROM TOP LEADERS IN OUR COMMUNITY

Recent Episodes

- Carsten Fischer: The Need for Speed in Threat Mitigation
- Stephen Sparkes: The Evolution of the CISO Role
- Lindsey Bateman: Keep Your Eyes On The Horizon For Emerging Threats – And New Solutions
- Burim Bivolaku: Financial Sector Collaboration Is Key To Third-Party Risk Management
- Beate Zwijnenberg: Can Cyber Risk be Quantified?
- Josh Magri: The CRI Profile – A Simplified Approach To Better Assessment
- Phil Venables: AI in Cybersecurity - Threats, Toil, and Talent

UPCOMING EVENTS

Americas

- 24 February | February Monthly CIAC Webinar
- 26 February | Member Success Session for New IntelX Users
- 9-12 March 2025 | Americas Spring Summit
- 30 April | CIAC Open Forum for Everyone
- 14 May | Member Community Connection, Los Angeles FBI
- 3 June 2025 | FinCyber Today Canada

View all Americas events.

TLP GREEN

12120 Sunset Hills Rd, Reston
VA 20190