TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	29/1/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 29 January 2026

8	7	2	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Recent Threat campaigns within financial institutions	Actively Exploited & Critical Vulnerabilities	Major Compromises and breaches	Threat actor activities in the UAE & Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a surge in sophisticated phishing, malware, and vulnerability-exploitation campaigns targeting enterprises across multiple sectors. Threat actors leveraged advanced techniques from AiTM phishing and vishing kits to AI-generated backdoors, DLL side-loading, supply-chain tampering, and unauthorized SSO abuse to compromise user accounts, developer environments, and enterprise systems. High-impact vulnerabilities affecting Cisco, Fortinet, Azure, Zoom, Chrome, Oracle, and GitLab further underscore the breadth of risks facing organizations. For the financial sector, the overarching theme is the exploitation of identity, authentication, and software-supply-chain weaknesses, with notable incidents impacting blockchain infrastructure and exposing sensitive personal information. Financial institutions should prioritize strong authentication, rapid patching, continuous monitoring, and enhanced developer-security hygiene. Strengthening incident response readiness and reinforcing governance around digital assets, cloud services, and third-party software remain critical to reducing exposure and ensuring operational resilience.

ADGM THREAT INTELLIGENCE SUMMARY

Multi-Stage AiTM Phishing Campaign Exploits SharePoint to Compromise User Accounts [Campaign] [High]

Custom Phishing Kits Enhance Vishing Campaigns Targeting Financial Services [Campaign] [High]

KONNI Campaign Targets Software Developers with AI-Generated PowerShell Backdoors [Campaign] [High]

Threat Actors Exploit Microsoft Visual Studio Code in Recruitment Lure Campaign [Campaign] [Medium]

New Infostealer Campaign Targets Users via Spoofed Software Installers [Campaign] [Medium]

MacSync Campaign Targets macOS Users with Infostealer and Trojanized Wallet Apps [Campaign] [Medium]

PDFSIDER Malware Campaign Targets Fortune 100 Corporation with DLL Side-Loading [Campaign] [Medium]

Malicious PyPI Package Impersonates SymPy to Deliver Crypto mining Malware [Campaign] [Medium]

Critical Remote Code Execution Vulnerability in Cisco Products Actively Exploited [Vulnerability] [High]

Active Exploitation of Fortinet FortiGate Devices via Unauthorized SSO [Vulnerability] [High]

High-Severity Vulnerability in Azure Windows Admin Centre Allows Remote Code Execution [Vulnerability] [Medium]

Critical Command Injection Vulnerability Disclosed in Zoom Node Multimedia Routers [Vulnerability] [Medium]

High-Severity Vulnerability in Google Chrome's V8 Engine [Vulnerability] [Medium]

Oracle Releases Critical Patch Update Addressing Vulnerabilities Across Multiple Product Families [Vulnerability] [Medium]

GitLab Releases Critical Security Patch Addressing Multiple Vulnerabilities [Vulnerability] [Medium]

SagaEVM Chain Experiences Security Incident Resulting in $7 Million in Withdrawals [Cyber Breach] [High]

Chatham Asset Management Investigates Cybersecurity Breach [Cyber Breach] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multi-Stage AiTM Phishing Campaign Exploits SharePoint to Compromise User Accounts	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Microsoft Defender Security Research Team has uncovered a multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) campaign targeting multiple organizations, particularly in the energy sector. This campaign exploits SharePoint file-sharing services to deliver phishing payloads and creates inbox rules to maintain persistence and evade detection. The attack escalates through a series of AiTM attacks and follow-on BEC activities, leading to significant account compromises.

This incident is critical for the financial services sector as it highlights the operational complexities of AiTM campaigns and the inadequacy of standard identity compromise responses. Organizations must recognize that simple password resets are insufficient; they need to revoke active session cookies and remove malicious inbox rules to effectively mitigate the threat posed by such sophisticated attacks.

Technical Details

- The campaign begins with initial access via a phishing email from a trusted vendor, likely compromised beforehand.
- Attackers use a SharePoint URL that requires user authentication, mimicking legitimate document-sharing workflows to enhance credibility.
- Users clicking the malicious URL are redirected to a credential prompt, obscuring visibility into the attack flow.
- In addition to user credentials, the threat actor is also stealing active session cookies. Using these stolen session cookies, the attacker is able to authenticate and access the victim's mailbox.
- An inbox rule is created to delete incoming emails and mark them as read, ensuring the victim remains unaware.
- The attackers launch a large-scale phishing campaign, sending over 600 emails to contacts within and outside the organization.
- They monitor the victim's mailbox for undelivered emails and delete them to maintain operational secrecy.
- Recipients of phishing emails who click the malicious link are subsequently targeted by additional AiTM attacks.
- The complexity of AiTM attacks necessitates advanced detection and response mechanisms beyond traditional methods.

Recommendations

- Enable MFA and Conditional Access policies in Microsoft Entra, focusing on risk-based access controls.
- Implement continuous access evaluation to monitor and manage user sessions effectively.
- Utilize advanced anti-phishing solutions to scan incoming emails and detect malicious links.
- Educate users on the risks associated with secure file sharing and phishing emails from trusted sources.
- Regularly monitor for suspicious activities and investigate sign-in attempts with unusual characteristics.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Custom Phishing Kits Enhance Vishing Campaigns Targeting Financial Services	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Okta Threat Intelligence has identified multiple custom phishing kits designed for voice-based social engineering, particularly in vishing campaigns. These kits are increasingly utilized by threat actors targeting organizations that rely on identity and access management platforms, including those in the cryptocurrency services. The kits allow attackers to intercept user credentials and manipulate the authentication flow in real-time, effectively bypassing multi-factor authentication (MFA) controls.

The emergence of these sophisticated phishing kits poses significant risks to the financial services sector, as they enable attackers to exploit vulnerabilities in identity authentication technologies. The ability to synchronize phishing tactics with verbal instructions during phone calls enhances the effectiveness of these attacks, potentially leading to unauthorized access and data breaches. Financial institutions must remain vigilant and adopt robust security measures to mitigate these evolving threats.

Technical Details

- Custom phishing kits are offered as a service and are tailored for voice-based social engineering attacks.
- Attackers can intercept user credentials and manipulate the authentication flow in real-time during phone interactions.
- The kits allow for dynamic control of the phishing pages presented to users, aligning with the caller's script.

- Attackers perform reconnaissance to gather information on targets, including usernames and commonly used applications.
- The phishing attack sequence involves spoofing company phone numbers and convincing users to navigate to phishing sites.
- Credentials entered by users are forwarded to the attacker's Telegram channel for immediate use.
- Real-time session orchestration enables attackers to prompt users for MFA challenges, such as OTPs or push notifications.
- The kits can bypass MFA methods that are not phishing-resistant, including push notifications with number matching.
- The trend indicates a growing market for vishing expertise and bespoke phishing tools tailored to specific services.
- Financial institutions must recognize the evolving nature of these threats to implement effective defenses.

Recommendations

- Enforce phishing-resistant authentication methods for all users.
- Implement network zones and tenant access control lists to restrict access from anonymizing services used by attackers.
- Educate employees on recognizing vishing attempts and the importance of verifying caller identities.
- Consider deploying live caller checks to confirm the legitimacy of phone interactions with users.
- Regularly review and update security protocols to address emerging threats and vulnerabilities.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
KONNI Campaign Targets Software Developers with AI-Generated PowerShell Backdoors	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Checkpoint has identified an ongoing phishing campaign linked to the North Korean threat actor KONNI, which is now targeting software developers and engineering teams, particularly those involved in blockchain and cryptocurrency. The attackers utilize AI-generated PowerShell backdoors, indicating an evolution in their tactics and tools.

This campaign is significant for the financial services sector as it highlights the increasing sophistication of cyber threats targeting development environments. By compromising these environments, attackers can gain

access to sensitive blockchain-related resources and infrastructure, posing a substantial risk to organizations involved in financial services, investment banking, and fintech.

Technical Details

- The campaign employs phishing techniques with lure documents designed to resemble legitimate project documentation related to blockchain and cryptocurrency.
- The infection chain begins with a Discord-hosted link that downloads a ZIP archive containing a PDF lure and a Windows shortcut (LNK) file.
- The LNK file executes an embedded PowerShell loader that extracts additional files, including a PowerShell backdoor and batch file.
- The PowerShell backdoor is obfuscated using arithmetic-based character encoding, complicating analysis, and detection.
- Anti-analysis checks are implemented to avoid detection by security tools, including monitoring for mouse activity and sandbox environments.
- The backdoor establishes persistence by creating a scheduled task disguised as a legitimate OneDrive startup task.
- The malware communicates with a Command and Control (C2) server using a JavaScript challenge emulation to bypass non-browser traffic filters.
- The use of AI in the development of the PowerShell backdoor reflects a notable shift in KONNI's operational capabilities.
- The campaign shows broader targeting across the APAC region, extending beyond KONNI's historical focus on South Korea.
- The overall objective appears to be to compromise development environments for access to sensitive assets, including cryptocurrency holdings.

Recommendations

- Implement robust email filtering and phishing detection mechanisms to block malicious communications.
- Educate software development teams about the risks of phishing and the importance of verifying the authenticity of project documentation.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by such malware.
- Employ endpoint detection and response (EDR) solutions to monitor for suspicious activities and malware behavior.
- Establish a response plan for incidents involving potential compromise of development environments, including immediate isolation and forensic analysis.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Threat Actors Exploit Microsoft Visual Studio Code in Recruitment Lure Campaign	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Jamf Threat Labs has identified an evolution in the Contagious Interview campaign, attributed to a North Korean threat actor. This campaign exploits Microsoft Visual Studio Code by using malicious task configuration files to execute harmful payloads on victim systems, often under the guise of recruitment or technical assignments.

The implications for the financial services sector are significant, as developers may inadvertently expose sensitive systems to compromise through seemingly legitimate repositories. This highlights the need for heightened vigilance when interacting with third-party code and repositories, particularly in environments handling financial data.

Technical Details

- The infection begins when a victim clones a malicious Git repository, often under recruitment pretenses, using Visual Studio Code.
- Trusting the repository author allows the execution of commands embedded in the tasks.json configuration file.
- On macOS, a shell command retrieves a JavaScript payload remotely, executing it independently of the Visual Studio Code process.
- The JavaScript payload, hosted on vercel[.]app, implements a backdoor that enables remote code execution and system fingerprinting.
- The backdoor establishes persistent communication with a command-and-control (C2) server, polling for instructions every five seconds.
- The payload collects host information, including system hostname and MAC addresses, for reconnaissance.
- It dynamically executes arbitrary JavaScript code supplied by the attacker, allowing for further exploitation.
- The backdoor can execute additional JavaScript instructions retrieved from the C2 server, maintaining its functionality over time.
- The campaign shows an evolution in techniques, integrating with legitimate developer workflows to evade detection.

Recommendations

- Ensure Threat Prevention and Advanced Threat Controls are enabled and set to block mode in security solutions.
- Developers should exercise caution when interacting with third-party repositories, especially those from unfamiliar sources.

- Review repository contents before marking them as trusted in Visual Studio Code.
- Vet projects thoroughly before executing "npm install," paying close attention to package[.]json files and install scripts.
- Implement regular training for developers on secure coding practices and recognizing potential threats.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
New Infostealer Campaign Targets Users via Spoofed Software Installers	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at VirusTotal have identified a new infostealer campaign that operates through spoofed software installers, specifically targeting users with ZIP files masquerading as legitimate software from MalwareBytes. The campaign employs a DLL sideloading technique, where a malicious DLL is executed alongside a trusted executable, leading to the installation of secondary stage infostealers designed to exfiltrate sensitive information.

This campaign poses significant risks to the financial services sector, as the infostealers are capable of harvesting credentials and cryptocurrency wallet information. The use of trusted software names to lure victims increases the likelihood of successful infections, making it crucial for financial institutions to enhance their detection and response capabilities against such sophisticated threats.

Technical Details

- The campaign utilizes ZIP files named similarly to MalwareBytes software.
- Each ZIP file contains a malicious DLL named "CoreMessaging.dll" and a TXT file with a GitHub URL, which aids in infrastructure mapping.
- DLL sideloading is employed to execute the malicious payload when the legitimate executable is run.
- The malicious DLLs exhibit unique metadata characteristics, which can be used for identifying related variants.
- Analysts can track malicious DLLs using specific signature strings found in the file metadata.
- The exported functions within these DLLs contain unusual alphanumeric strings that serve as indicators for related malicious components.
- The campaign's secondary payloads are primarily infostealers, flagged by YARA rules for stealing cryptocurrency wallet browser extension IDs.
- A specific behash identifier can be used to pivot and uncover additional variants of the infostealers.

- The campaign was active between January 11 and January 15, 2026.

Recommendations

- Implement robust endpoint detection and response solutions to identify and block DLL sideloading attempts.
- Conduct regular training for employees on recognizing spoofed software and phishing attempts.
- Utilize threat intelligence feeds to stay updated on emerging Infostealer campaigns and their indicators of compromise.
- Monitor network traffic for unusual data exfiltration patterns, particularly related to cryptocurrency transactions.
- Regularly audit and update software to ensure that only legitimate applications are installed and run on systems.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
MacSync Campaign Targets macOS Users with Infostealer and Trojanized Wallet Apps	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at CloudSEK have identified a new macOS Infostealer named MacSync, which is delivered through a ClickFix-style phishing lure. This campaign tricks users into executing a Terminal command that compromises their systems, harvesting sensitive data such as passwords and cryptocurrency wallet information. The malware also trojanizes trusted hardware wallet applications, transforming them into long-term phishing tools.

The implications for the financial services sector are significant, as MacSync specifically targets cryptocurrency users, making it a serious threat to digital asset security. The stealthy nature of the attack, combined with the exploitation of user trust in legitimate applications, underscores the need for heightened awareness and robust security measures among financial institutions involved in cryptocurrency transactions.

Technical Details

- MacSync is delivered via a phishing lure that mimics a legitimate macOS cloud storage installer, tricking users into executing a malicious Terminal command.
- The malware operates through a multi-stage infection process, utilizing a daemonized Zsh stager to retrieve and execute a remote AppleScript payload.

- It systematically harvests browser credentials, cryptocurrency wallet data, and sensitive files by phishing the victim's macOS system password through fake dialogs.
- The malware can trojanize popular Electron-based cryptocurrency applications, such as Ledger and Trezor, by overwriting critical components to create a persistent threat.
- The supporting infrastructure includes multiple rotating command and control (C2) domains, indicating an ongoing and evolving campaign.
- The infection process exploits user trust in macOS installation workflows, bypassing traditional security measures like Gatekeeper and notarization checks.
- The payload employs obfuscation techniques, making static analysis difficult and evading basic signature-based detection.
- MacSync prioritizes the theft of cryptocurrency-related data, targeting known wallet directories and browser profiles for sensitive information.
- The trojanized applications present convincing phishing interfaces to capture device PINs and recovery phrases from unsuspecting users.
- The campaign demonstrates a clear focus on maximizing yield from cryptocurrency users, highlighting the need for enhanced security awareness.

Recommendations

- Educate users about the risks of executing commands from untrusted sources, emphasizing the dangers of pasting commands into Terminal.
- Implement robust endpoint protection solutions that can detect and block malicious scripts and unauthorized application modifications.
- Monitor for unusual activity related to cryptocurrency wallets and browser profiles, focusing on data exfiltration attempts.
- Block known malicious domains associated with the MacSync campaign at the network level to prevent initial infection.
- Regularly update and patch software to mitigate vulnerabilities that could be exploited by similar campaigns.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
PDFSIDER Malware Campaign Targets Fortune 100 Corporation with DLL Side-Loading	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

PDFSIDER, a newly identified malware variant, has been deployed through DLL side-loading techniques, specifically targeting Windows endpoints of a Fortune 100 corporation. The malware utilizes a fake cryptbase.dll to bypass endpoint detection systems, allowing for covert backdoor access and encrypted command-and-control communications.

This incident is significant for the financial services sector as it highlights the evolving tactics of advanced persistent threats (APTs) that blend traditional cyber-espionage with modern remote-command functionalities. The use of DLL side-loading to evade detection poses a serious risk, as it can be exploited by sophisticated actors to gain unauthorized access to sensitive systems, making it essential for organizations to enhance their security measures.

Technical Details

- PDFSIDER is delivered via spear-phishing emails containing a ZIP archive with a legitimate EXE file, which is executed by the victim.
- The malware employs DLL side-loading, where a malicious DLL is loaded instead of the legitimate cryptbase.dll, granting code execution.
- Once executed, PDFSIDER initializes Winsock and establishes encrypted communications with its command-and-control server.
- The malware operates primarily in memory, minimizing disk artifacts and ensuring stealthy execution.
- It creates anonymous pipes to execute commands using cmd.exe without displaying a console window.
- PDFSIDER uses the Botan cryptographic library for AES-256-GCM encryption, securing all inbound and outbound data.
- The malware includes anti-VM checks to avoid execution in virtualized environments, enhancing its evasion capabilities.
- Threat actors may use decoys to lure victims, including fake documents that appear legitimate.
- The campaign has shown a trend of targeting high-profile organizations, utilizing social engineering tactics to gain access.
- PDFSIDER is interpreted as a tradecraft for targeted attacks rather than mass-scale malware distribution.

Recommendations

- Implement robust email filtering to detect and block spear-phishing attempts.
- Regularly update and patch software to mitigate vulnerabilities that can be exploited for DLL side-loading.

- Employ endpoint detection and response (EDR) solutions that can identify and block suspicious DLL loading activities.
- Conduct regular security awareness training for employees to recognize social engineering tactics.
- Monitor network traffic for unusual, encrypted communications indicative of command-and-control activity.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – PDFSIDER Malware Campaign

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Malicious PyPI Package Impersonates SymPy to Deliver Crypto mining Malware	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Socket's Threat Research Team identified a malicious PyPI package named sympy-dev that impersonates the legitimate SymPy library, which has approximately 85 million downloads per month. This malicious package contains a downloader and executes crypto mining malware upon invocation of specific polynomial functions, increasing the risk of accidental installation among developers.

The presence of this malware is particularly concerning for the financial services sector, as it highlights the vulnerabilities associated with software supply chains and the potential for unauthorized resource hijacking. The ability of this malware to execute in-memory reduces traditional detection methods, making it a significant threat to environments that utilize Python for data processing and analysis.

Technical Details

- The malicious package sympy-dev was designed to mimic the legitimate SymPy library, increasing the likelihood of accidental installation.
- It contains a downloader that retrieves a remote JSON configuration and a threat actor-controlled ELF payload.
- The payload is executed in-memory using Linux functions memfd_create and /proc/self/fd, minimizing disk artifacts.
- The malware primarily functions as an XMRig crypto miner, directing mining operations to threat actor-controlled Stratum endpoints over TLS.
- The package has four releases, all containing malicious code, and was downloaded over 1,000 times within its first day on PyPI.

- The execution chain activates when specific polynomial routines are invoked, blending into normal SymPy usage patterns.
- The threat actor's infrastructure includes two command and control (C2) endpoints for payload retrieval.
- The malware loader can fetch and execute arbitrary second-stage code, posing a broader risk beyond crypto mining.
- The malicious code suppresses errors to maintain normal behavior, complicating detection efforts.
- The campaign illustrates the ongoing risk of typo squatting in software repositories, which can lead to significant security breaches.

Recommendations

- Implement strict dependency pinning and integrity checks in software builds to prevent the use of malicious packages.
- Restrict installations to vetted package indexes or internal mirrors to mitigate the risk of typo squatting.
- Monitor Python processes for unexpected outbound requests or in-memory executions to detect potential malware activity.
- Educate developers on the risks associated with package installations and the importance of verifying package authenticity.
- Utilize automated tools to flag and block known malicious packages before they are fetched by package managers.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Malicious PyPI Package

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Code Execution Vulnerability in Cisco Products Actively Exploited	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Cisco has issued an urgent security advisory regarding a critical Remote Code Execution (RCE) vulnerability, tracked as CVE-2026-20045, which is actively being exploited in the wild. This vulnerability affects several core Cisco enterprise communications platforms, including Unified Communications Manager and Cisco

Unity Connection, allowing unauthenticated remote attackers to gain root-level access to the underlying operating system.

This vulnerability poses significant risks to the financial services sector, as successful exploitation can lead to service disruption, interception of communications, and complete infrastructure takeover. Organizations utilizing affected Cisco products must prioritize immediate remediation actions to mitigate the potential impacts of this vulnerability.

Technical Details

- CVE-2026-20045 is classified as a critical Remote Code Execution (RCE) vulnerability with confirmed active exploitation.
- The vulnerability arises from improper validation and sanitization of user-supplied input in HTTP requests.
- Attackers can gain unauthenticated user-level access, escalating privileges to root, and achieving full control over affected devices.
- Potential impacts include interruption of voice and messaging services, unauthorized access to call data, and lateral movement into internal networks.
- Exploitation can lead to the deployment of malware or ransomware, resulting in long-term compromise.
- The vulnerability affects various components within Cisco Unified Communications Manager, Unity Connection, and Webex Calling
- The vulnerability affects Cisco Unified CM, Unified CM IM&P, Unified CM SME, Cisco Unity Connection Release, and Webex Calling.
- Cisco has elevated the risk rating to Critical due to the severity of the exploitation potential.
- Immediate remediation actions are strongly advised to prevent exploitation.
- Fixed version includes:

Cisco Unified CM, Unified CM IM&P, Unified CM SME, Cisco Unity Connection Release, and Webex Calling Dedicated Instance Release	First Fixed Release
12.5	Migrate to a fixed release.
14	14SU5 or apply patches
15	15SU4 (Mar 2026) or apply patches

Recommendations

- Apply Cisco Security Updates immediately to mitigate the vulnerability.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Active Exploitation of Fortinet FortiGate Devices via Unauthorized SSO	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Security researchers have identified an active and ongoing malicious campaign targeting Fortinet FortiGate firewall devices through unauthorized Single Sign-On (SSO) administrator access. Threat actors are leveraging malicious SSO logins to gain administrative access, exfiltrate firewall configurations, create persistent administrative accounts, and modify VPN access settings.

This activity poses a significant risk to enterprise perimeter security, particularly for organizations operating FortiGate devices. The campaign demonstrates a high degree of automation and persistence techniques, indicating that existing patches may not fully mitigate the threat. Immediate defensive action is advised for affected organizations.

Technical Details

- Malicious access is achieved via SSO-based administrator logins, likely exploiting weaknesses in FortiCloud SSO authentication.
- The activity mirrors prior exploitation of crafted SAML messages that allow authentication bypass when FortiCloud SSO is enabled.
- Login attempts originate from a limited set of external hosting providers, suggesting centralized attacker infrastructure.
- Once administrative access is obtained, actions occur within seconds, starting with a successful SSO administrator login.
- Commonly observed login accounts use generic email-style formats, indicating potential automation.
- Full system configuration can be downloaded via the FortiGate GUI, enabling offline analysis and credential hash cracking.
- Secondary administrator accounts with super_admin privileges are created to establish persistence.
- Newly created accounts may grant VPN access, allowing long-term unauthorized access.
- The campaign is linked to previously disclosed Fortinet authentication bypass vulnerabilities (CVE-2025-59718 and CVE-2025-59719).
- While Fortinet released patches addressing these vulnerabilities, it is currently unclear whether the latest observed activity is fully mitigated by existing fixes.

Recommendations

- Closely monitor Fortinet advisories and firmware releases, applying all relevant security patches immediately.
- If any IOC activity is detected, reset all local and SSO-linked administrative credentials and enforce strong, unique passwords.

- Conduct a full audit of system.admin objects and VPN user mappings, removing any unknown or suspicious accounts.
- Limit FortiGate management access to trusted internal IP ranges and disable public exposure of management interfaces.
- Consider temporarily disabling FortiCloud SSO due to its strong correlation with SSO abuse.

For the indicators of compromise (IOCs), refer to the attached CSV sheet.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerability in Azure Windows Admin Center Allows Remote Code Execution	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Security researchers have identified a high-severity vulnerability in the Azure Active Directory Single Sign-On implementation of Microsoft Windows Admin Center. This flaw arises from improper verification of cryptographic signatures during token validation, allowing an attacker with local administrator access to bypass authentication and authorization controls.

This vulnerability is critical for the financial services sector as it could enable unauthorized access to sensitive systems and data, potentially leading to significant financial losses and reputational damage. Organizations utilizing Azure Windows Admin Center must prioritize remediation to safeguard their environments against potential exploitation.

Technical Details

- The vulnerability is classified under CVE ID: CVE-2026-20965, with a CVSS score of 7.5.
- It is categorized as an Elevation of Privilege vulnerability, allowing attackers to gain higher access levels.
- The weakness is classified as CWE-347, indicating improper verification of cryptographic signatures.
- Affected systems include the Azure AD SSO authentication flow within the Windows Admin Center Azure Extension.
- Attackers with local administrator access can exploit this vulnerability to bypass security controls.
- A fixed version of the Windows Admin Center Azure Extension is available, specifically version 0.70.00 or later.
- Continuous monitoring and vulnerability management practices are essential to prevent exploitation.

Recommendations

- Upgrade the Windows Admin Center Azure Extension to version 0.70.00 or later to address the vulnerability.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Command Injection Vulnerability Disclosed in Zoom Node Multimedia Routers	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Zoom has disclosed a critical Command Injection vulnerability affecting Zoom Node Multimedia Routers (MMRs) used in hybrid and meeting connector deployments. The vulnerability, tracked as CVE-2026-22844, allows a malicious meeting participant to execute arbitrary commands remotely on a vulnerable MMR over the network, posing a significant risk to organizations utilizing these systems.

This flaw carries a CVSS v3.1 score of 9.9, indicating near-maximum severity. Organizations running Zoom Node Meetings Hybrid (ZMH) or Zoom Node Meeting Connector (MC) deployments with MMR versions prior to 5.2.1716.0 are immediately exposed and should prioritize remediation to mitigate potential system compromise.

Technical Details

- CVE ID: CVE-2026-22844, classified as a critical Command Injection vulnerability.
- CVSS Score of 9.9 indicates near-maximum severity and potential for significant impact.
- Vulnerability allows remote execution of arbitrary commands on vulnerable MMRs.
- Exploitation can occur without user interaction, increasing risk for organizations.
- Attack vector is network-based, requiring low-privilege access as a meeting participant.
- Affected products include MMR versions earlier than 5.2.1716.0 for both ZMH and MC deployments.
- Organizations are urged to upgrade to version 5.2.1716.0 or later to mitigate the risk.
- The flaw operates across a changed security scope, further exacerbating organizational vulnerabilities.
- Immediate action is recommended for organizations to protect their systems from potential exploitation.
- The vulnerability highlights the importance of maintaining updated software in critical communication tools.

Recommendations

- Upgrade all affected systems to the vendor-recommended fixed versions.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerability in Google Chrome's V8 Engine	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Google has released a security update for the Chrome browser to address a high-severity vulnerability affecting the V8 JavaScript engine. This flaw could allow attackers to exploit a race condition, potentially leading to unexpected behavior or security compromise within the browser.

This vulnerability is particularly concerning for the financial services sector, as successful exploitation may enable unauthorized actions, compromising sensitive user data and transactions. Financial institutions must ensure their systems are updated to mitigate the risks associated with this vulnerability.

Technical Details

- CVE-2026-1220 identifies a race condition in the V8 JavaScript engine, which is critical for executing JavaScript code in Chrome.
- The vulnerability arises from improper handling of concurrent operations, which can lead to unexpected behavior in the browser.
- Successful exploitation may allow attackers to perform unauthorized actions in the context of the browser, posing significant security risks.
- Google has released fixed versions for various platforms, including Windows, Mac, Linux, and Android.
- The stable channel update for desktop includes versions 144.0.7559.96/.97 for Windows/Mac and 144.0.7559.96 for Linux.
- An update for Chrome on Android is also available, version 144.0.7559.90.
- Chrome Stable 144 (144.0.7559.95) for iOS has been updated as well.

Recommendations

- Immediately update Google Chrome to the latest version to mitigate the identified vulnerability.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Oracle Releases Critical Patch Update Addressing Vulnerabilities Across Multiple Product Families	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Oracle has released its quarterly Critical Patch Update in January 2026, which addresses a total of 337 new

security vulnerabilities across over 30 product families, including critical systems in Financial Services. Among these vulnerabilities, 158 unique CVEs have been identified, with a significant portion being remotely exploitable without authentication, leading to potential unauthorized access and data manipulation.

The presence of critical vulnerabilities, including those with CVSS scores of 10.0, poses serious risks to financial institutions relying on Oracle products. The update highlights the importance of timely patch management in the financial sector to mitigate risks associated with unauthorized access and denial-of-service attacks.

Technical Details

- Oracle's January 2026 CPU addresses 337 vulnerabilities across multiple product families, including Database and Financial Services.
- The update includes 158 unique CVEs, with critical vulnerabilities making up about 8% of the total.
- High-severity vulnerabilities account for 45.7% of the update, indicating a significant risk level.
- Many vulnerabilities are remotely exploitable without authentication, increasing the risk of unauthorized access.
- Notable CVEs include CVE-2026-21962 and CVE-2025-66516, both with a CVSS score of 10.0.
- CVE-2025-49796 affects multiple Financial Services products, including Banking Branch and Cash Management.
- CVE-2026-21945 involves Server-Side Request Forgery (SSRF) vulnerabilities in Oracle Java SE.
- The vulnerabilities could lead to data manipulation and denial-of-service attacks.
- Financial institutions using affected Oracle products are urged to prioritize patching.
- The update emphasizes the need for continuous monitoring and vulnerability management.

Recommendations

- Implement the latest (January 2026) Oracle Critical Patch Update to address identified vulnerabilities.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
GitLab Releases Critical Security Patch Addressing Multiple Vulnerabilities	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

GitLab has released urgent security patch updates for both its Community Edition (CE) and Enterprise Edition (EE) to address multiple high- and medium-severity vulnerabilities. These vulnerabilities expose GitLab installations to Denial of Service (DoS) attacks and, in a critical case, a potential bypass of two-factor authentication (2FA).

The vulnerabilities are significant for the financial services sector as they could allow unauthorized access and service disruptions, impacting the integrity and availability of critical financial applications. Organizations using GitLab are urged to implement the patches promptly to mitigate these risks.

Technical Details

- CVE-2025-13927: A high-severity vulnerability allowing unauthenticated attackers to send crafted requests to the Jira Connect integration, resulting in a denial-of-service condition.
- CVE-2025-13928: High-severity flaw in the Releases API that could enable unauthenticated attackers to trigger denial of service conditions.
- CVE-2026-0723: A high-severity two-factor authentication bypass vulnerability that could allow attackers to bypass 2FA by submitting forged device responses.
- CVE-2025-13335: A medium-severity vulnerability that could lead to an infinite loop in Wiki redirects, causing denial of service for authenticated users.
- CVE-2026-1102: A medium-severity vulnerability allowing unauthenticated attackers to cause denial of service via malformed SSH authentication requests.
- Impacted versions include all GitLab CE/EE versions from 11.9 before 18.6.4, and various versions up to 18.8.2.
- Fixed versions include GitLab 18.8.2, 18.7.2, or 18.6.4.
- The vulnerabilities have been assigned CVSS scores ranging from 5.3 to 7.5, indicating their severity.

Recommendations

- Upgrade immediately to one of the patched versions: GitLab 18.8.2, 18.7.2, or 18.6.4.

Detailed Vulnerability Details and Affected Products can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
SagaEVM Chain Experiences Security Incident Resulting in $7 Million in Withdrawals	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

Saga, a blockchain entity, has identified a security incident affecting the SagaEVM chain, leading to significant liquidity withdrawals. The incident involved a coordinated sequence of contract deployments and cross-chain activities, prompting the suspension of the SagaEVM chain to mitigate further impact.

The financial services sector should be aware of this incident as it highlights vulnerabilities in blockchain infrastructure that can lead to substantial financial losses. The incident underscores the importance of robust security measures and rapid response protocols to protect digital assets and maintain trust in blockchain technologies.

Technical Details

- A coordinated security incident was confirmed on the SagaEVM chain, leading to a pause at block height 6593800.
- Nearly $7 million worth of assets, including USDC, yUSD, ETH, and tBTC, were transferred to the Ethereum Mainnet by the exploiters.
- The identified exploiter's wallet address is 0x2044697623afa31459642708c83f04ecef8c6ecb, which is being blacklisted by exchanges and bridges.
- No consensus failure, validator compromise, or signer key leakage has been reported, indicating the broader Saga network remains secure.
- Engineering teams are conducting a full forensic investigation using archive data and execution traces to validate the incident's impact.
- The SagaEVM chainlet will remain paused until the mitigation process is complete and risks are fully assessed.
- The incident emphasizes the need for ongoing vigilance and robust security practices in blockchain operations.

Recommendations

- Implement stringent monitoring of cross-chain activities to detect anomalies early.
- Enhance security protocols for contract deployments to prevent unauthorized access.
- Regularly review and update incident response plans to ensure rapid action during security breaches.
- Collaborate with exchanges to establish swift blacklisting procedures for identified malicious wallets.
- Conduct regular security audits and forensic analyses to strengthen infrastructure resilience.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Chatham Asset Management Investigates Cybersecurity Breach	MEDIUM	CLEAR	Cyber Breach	Open Source

Executive Summary

On January 20, 2026, Chatham Asset Management notified certain state regulators that it is investigating a cybersecurity incident involving unauthorized activity on its network, first identified on December 8, 2025. The breach potentially exposes sensitive personal information, including names, Social Security numbers, and driver's license numbers, raising significant concerns for affected individuals and stakeholders in the financial services sector.

The incident highlights the increasing importance of robust cybersecurity measures in the investment industry, where operational resilience is critical for maintaining trust and competitive advantage. As cyber

threats evolve, firms must prioritize data governance and incident response capabilities to safeguard sensitive information and uphold their reputations.

Technical Details

- Unauthorized activity was detected within Chatham's network, prompting immediate incident-response measures.
- The firm engaged outside cybersecurity specialists to investigate the breach and secure its systems.
- Public reports suggest that the breach may involve sensitive personally identifiable information (PII).
- The investigation is focused on whether any PII was accessed or exfiltrated during the incident.
- Ransomware-linked claims have been associated with the incident, specifically from a group named "Worldleaks."
- Affected information may include names, Social Security numbers, and driver's license numbers.
- The incident has triggered regulatory notifications in multiple states across US.
- Firms typically follow a sequence of steps for incident response, including containment, forensic review, and notification.

Recommendations

- Implement robust incident response plans that include regular tabletop exercises and third-party engagement.
- Enforce multi-factor authentication (MFA) across all critical systems to enhance access controls.
- Conduct regular audits of data governance and cybersecurity measures to identify vulnerabilities.
- Provide affected individuals with credit monitoring and identity restoration services following a breach.
- Foster a culture of cybersecurity awareness and training among employees to mitigate risks.

Reference to the Source

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

PDFSIDER Malware - Exploitation of DLL Side-Loading for AV and EDR Evasion

Tactic	Technique
Initial Access	T1574.002 - DLL Side-Loading
Execution	T1059.003 - Windows Command Shell
	T1204 - User Execution
Defense Evasion	T1497 - Virtualization/Sandbox Evasion
	T1622 - Debugger Evasion
Discovery	T1082 - System Information Discovery
Command & Control	T1095 - Non-Application Layer Protocol
	T1041 - Exfiltration Over C2 Channel
Execution	T1106 - Native API

PyPI Package Impersonates SymPy to Deliver Crypto mining Malware TTPs

T1195.002 — Supply Chain Compromise: Compromise Software Supply Chain

T1608.001 — Stage Capabilities: Upload Malware

T1204.005 — User Execution: Malicious Library

T1059.006 — Command and Scripting Interpreter: Python

T1036 — Masquerading

T1656 — Impersonation

T1105 — Ingress Tool Transfer

T1071.001 — Application Layer Protocol: Web Protocols

T1095 — Non-Application Layer Protocol

T1027.002 — Obfuscated Files or Information: Software Packing

T1496.001 — Resource Hijacking: Compute Hijacking

Appendix B – Threat Severity Ratings & Definitions

In this newsletter, each campaign, breach, and vulnerability has been assigned a severity level—High, Medium, or Low—based on a contextual assessment of its impact, relevance to the financial sector, regional exposure, and exploit status.

A **High** severity rating is assigned to threats that involve widely used technologies, nation-state actors, or actively exploited zero-day vulnerabilities. These incidents pose a significant risk due to their potential for widespread disruption, data compromise, and strategic targeting of core infrastructure.

A **Medium** severity rating reflects threats that are technically impactful but have limited regional exposure or affect less prominent entities. These may include ransomware attacks on mid-sized firms, blockchain-based malware delivery mechanisms, or smart contract exploits in DeFi platforms.

A **Low** severity rating is applied to threats that are peripherally related to the financial sector, have no confirmed impact in the region, or target non-critical systems. These include credential stuffing attacks on platforms outside the MENA region or supply chain breaches that have not yet affected local infrastructure.

Threat Score Ratings & Definitions

1. **Severe**: Widespread, high-impact attacks ongoing. Critical infrastructure affected by destructive malware or multiple zero-day exploits.
2. **High**: Confirmed breaches or coordinated campaigns in progress. High-impact threat actor activity and zero-day exploitation observed.
3. **Elevated**: Active exploitation of known vulnerabilities or targeted campaigns detected. Some breaches or zero-days may surface.
4. **Guarded**: Slight increase in malicious activity. Low-level campaigns or threat actor reconnaissance may be underway.
5. **Normal**: No significant cyber activity beyond baseline. No major breaches, campaigns, or zero-day activity observed.

Appendix C – Traffic Light Protocol (TLP) Definitions and Usage

TLP	When should it be used?	How should it be shared?
TLP:Red	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:Amber+Strict	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:Amber	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	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.
TLP:Green	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible

		channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:Clear	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Appendix D - Acronyms & Technical Terms

Term / Acronym	Meaning / Description
2FA (Two-Factor Authentication)	Security process requiring two independent authentication factors.
AES-256-GCM	Strong encryption algorithm used by malware for secure communications.
AiTM (Adversary-in-the-Middle)	A phishing technique where attackers intercept and manipulate authentication sessions between user and service.
Anonymous Pipes	Windows mechanism misused by malware for stealth command execution.
Azure AD	Microsoft cloud identity platform affected in authentication vulnerabilities.
Backdoor	Malicious program that allows attackers secret remote access to a system.
BEC (Business Email Compromise)	Fraud involving unauthorized access to business email accounts to redirect payments or manipulate communications.
Botan Library	Cryptographic library used by malware for encrypted communication.
C2 (Command and Control)	Servers attackers use to send instructions to infected computers.
Chatham Asset Management	Financial firm impacted by a cybersecurity breach.
Chrome Stable Channel	Official release branch of Google Chrome providing security updates.
ClickFix-style Phishing	macOS phishing method tricking users into running terminal commands.
Command Injection	Attack where an adversary forces a system to execute unauthorized commands.
Conditional Access	Security policies that determine when users are allowed to access applications based on risk.
Crypto miner	Malware that hijacks system resources to mine cryptocurrency.
CSC	UAE Cyber Security Council
CVE	Identifier assigned to publicly known vulnerabilities.
CVSS	Scoring system for rating vulnerability severity.
CWE-347	Weakness type describing failures in verifying cryptographic signatures.
Discord-hosted Link	Malicious download link stored on Discord infrastructure.
DLL Sideloading	Technique where a malicious DLL is loaded instead of a legitimate one.
DoS (Denial of Service)	Attack aiming to disrupt service availability.
Electron-based Wallet Apps	Crypto wallet applications built on Electron framework that can be trojanized.
Forensic Investigation	Deep analysis performed after a breach to determine cause and impact.
FortiCloud SSO	SSO mechanism used in Fortinet devices and abused in attacks.
FortiGate	Firewall device targeted through unauthorized SSO access.
Git Repository	Code storage location that attackers can tamper with to spread malware.
Inbox Rules	Automated email filters that attackers abuse to hide their presence.
Infostealer	Malware designed to steal credentials files or wallet information.

JavaScript Payload	Malicious JavaScript code executed on a compromised machine.
Jira Connect Integration	GitLab component affected by DoS vulnerability.
KONNI	North Korean threat actor group known for espionage-focused malware campaigns.
LNK File	Windows shortcut file that can execute embedded commands and start malware.
MacSync	New macOS Infostealer targeting crypto users.
memfd_create	Linux function allowing execution of malware in memory without touching disk.
MFA (Multi-Factor Authentication)	Additional identity verification beyond passwords to strengthen security.
Microsoft Defender XDR	Microsoft's extended detection and response platform that identifies suspicious activities across systems.
MMR (Multimedia Router)	Zoom infrastructure component vulnerable to command injection.
Okta FastPass	Phishing-resistant authentication method offered by Okta.
Oracle CPU (Critical Patch Update)	Quarterly Oracle release addressing hundreds of vulnerabilities.
PDFSIDER	Malware variant using DLL sideloading against enterprise endpoints.
Phishing Kits	Pre-built tools that attackers use to create fake login pages and harvest credentials.
PII (Personally Identifiable Information)	Sensitive information such as SSNs or driver's license numbers.
PowerShell Backdoor	Malicious script that provides remote unauthorized control on Windows systems.
PyPI	Python Package Index where malicious Python packages can be uploaded.
Race Condition	Software bug caused by improper handling of simultaneous operations.
RCE (Remote Code Execution)	Ability for an attacker to run commands on a remote system.
Saga Network	Blockchain platform affected by a major security incident.
SagaEVM	Blockchain environment that experienced $7M unauthorized withdrawals.
SAML	Authentication standard that can be manipulated for unauthorized access.
Scheduled Task	Windows automation mechanism often misused for persistence.
Server-Side Request Forgery (SSRF)	Attack letting adversaries force servers to make internal network requests.
SharePoint	Microsoft's enterprise document sharing system used by attackers to deliver phishing links.
SSO (Single Sign-On)	Central login mechanism that attackers target to gain broad access.
SSRF (Server-Side Request Forgery)	Vulnerability that lets attackers trick servers into making unauthorized requests.
Stratum Endpoints	Servers used for directing cryptocurrency mining traffic.
Super_Admin	Highest privileged FortiGate account created by attackers for persistence.
Sympy-dev	Malicious Python package impersonating the real SymPy library.
tasks[.]json	VS Code configuration file that can execute attacker-controlled commands.
Trojanized Application	Legitimate software modified to steal data.
Typo squatting	Tricking users by uploading malicious packages with names similar to real packages.
USDC	yUSD, ETH, tBTC : Cryptocurrency assets stolen in the Saga blockchain incident.
V8 JavaScript Engine	Chrome component vulnerable to exploitation.
Vishing	Voice-based social engineering attacks conducted over phone calls.
Visual Studio Code (VS Code)	Developer tool exploited to run malicious tasks from untrusted repositories.
Worldleaks	Ransomware-linked group claiming involvement in a data breach.
XMRig	Popular crypto mining software often used in malware.
YARA Rule	Pattern used by security teams to detect malware families.
Zoom Node Meeting Connector	Zoom deployment type affected by MMR vulnerability.

Zsh Stager	macOS script used to stage and retrieve additional malware.