TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	19/2/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 19 February 2026

7	6	1	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Finance Sector	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 wave of social engineering that uses deepfake video, fake recruiter outreach, trusted discussion forums, and phishing attachments to deliver remote access tools, information stealers, and ransomware. Key campaigns include UNC1069 focused on crypto, a newly observed actor UAT 9921 using the VoidLink framework, XWorm delivered through malicious Excel files, abuse of Google Groups that installs Lumma and a rogue Linux browser, and Lazarus activity that lures developers with public package repositories. Researchers also noted a ClickFix method that uses custom DNS requests to stage follow on payloads, and the Phorpiex botnet pushing GLOBAL GROUP ransomware that can operate without talking to external servers. On the vulnerability front, there are active exploits in Chrome and Apple devices, a critical issue in the React Native Community tools that affects developer machines, multiple zero-day issues in the February Microsoft update, and additional weaknesses in Ivanti and Fortinet products. For financial institutions, immediate risks are account takeover, compromise of development environments, and exposure of client data, as shown by the Figure Technology incident driven by social engineering. It is recommended to apply current security updates for Chrome, Apple, and Microsoft, update Ivanti and Fortinet where used, strengthen sign in protections and staff awareness, improve device monitoring for employees and contractors, reduce development risk by allowing only approved packages, limit access to build and test systems, monitor for unusual network requests and ransomware that operates without outside contact, and tighten oversight of single sign on providers.

ADGM THREAT INTELLIGENCE SUMMARY

UNC1069 Targets Digital-Asset Ecosystem with AI-Enabled Social Engineering [Campaign] [High]

New Threat Actor UAT-9921 Leverages VoidLink Framework in Cyber Campaigns [Campaign] [High]

New XWorm Campaign Utilizing Multiple-Themed Phishing Emails [Campaign] [High]

Cybercriminals Exploit Google Groups to Distribute Lumma Info-Stealer and Ninja Browser Malware [Campaign] [High]

Lazarus Group's "Graphalgo" Campaign Targets Crypto Developers with RAT [Campaign] [Medium]

New Attack Campaign Utilizing ClickFix Technique Targets Users with Custom DNS Lookups [Campaign] [Medium]

Phorpiex Phishing Campaign Delivers GLOBAL GROUP Ransomware [Campaign] [Medium]

Active Exploitation of Zero-Day Vulnerability CVE-2026-2441 in Google Chrome [Vulnerability] [High]

Critical Vulnerability in Apple Products Allows Arbitrary Code Execution [Vulnerability] [High]

Critical Remote Code Execution Vulnerability in React Native Community CLI Actively Exploited [Vulnerability] [High]

Microsoft February 2026 Patch Tuesday Security Update Addresses Multiple Critical Vulnerabilities [Vulnerability] [High]

Multiple Vulnerabilities in Ivanti Endpoint Manager Expose Sensitive Data [Vulnerability] [Medium]

Multiple Vulnerabilities Identified in Fortinet Products [Vulnerability] [Medium]

Figure Technology Suffers Data Breach Exposing Customer Information [Cyber Breach] [High]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
UNC1069 Targets Digital-Asset Ecosystem with AI-Enabled Social Engineering	HIGH	CLEAR	Campaign	Open Source

Executive Summary

UNC1069, a financially motivated North Korean threat actor, has been identified targeting the digital-asset ecosystem through sophisticated social-engineering tactics. The group has deployed multiple malware families, including SILENCELIFT, DEEPBREATH, and CHROMEPUSH, utilizing compromised accounts and AI-generated content to deceive victims into executing malicious commands.

This campaign suggests an ongoing evolution in financially motivated threats, where advanced social engineering, AI-assisted tooling, and tailored malware could be used to enable theft. While the overall impact on financial services remains under assessment, firms with exposure to cryptocurrency and decentralized finance may experience elevated risk.

Technical Details

- The attack began with a compromised Telegram account, leading to a fake Zoom meeting where victims were deceived using a deepfake video.
- Victims executed commands under the guise of troubleshooting, initiating the infection chain on their systems.
- The malware deployed includes WAVESHAPER, a backdoor that facilitates further payload delivery.
- HYPERCALL, a downloader, retrieves additional malware from command-and-control servers.
- DEEPBREATH manipulates macOS's TCC database to gain unauthorized access to sensitive data.
- CHROMEPUSH installs as a browser extension, capturing keystrokes and browser cookies.
- The attack showcases a high volume of tooling on a single host, indicating a targeted approach to data harvesting.
- Persistence mechanisms were established through launch daemons to ensure malware execution at startup.
- The incident underscores the potential for identity theft and future social engineering campaigns using harvested data.
- UNC1069's tactics reflect a significant evolution in their operational capabilities, focusing on the digital asset ecosystem including crypto.

Recommendations

- Implement multi-factor authentication (MFA) to secure accounts against unauthorized access.
- Conduct regular training for employees on recognizing social engineering tactics and phishing attempts.
- Monitor network traffic for unusual activity indicative of malware communication with command-and-control servers.
- Employ endpoint detection and response (EDR) solutions to identify and mitigate malware threats.
- Regularly update and patch systems to protect against known vulnerabilities exploited by malware.

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 Threat Actor UAT-9921 Leverages VoidLink Framework in Cyber Campaigns	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Cisco Talos has identified a new threat actor, UAT-9921, utilizing the VoidLink framework in their cyber campaigns. This actor has been active since at least 2019 and employs compromised hosts to install VoidLink command and control (C2) systems, enabling them to conduct internal and external network reconnaissance. The VoidLink framework features a modular design that specifically targets Linux systems, allowing for advanced implant management capabilities.

The emergence of UAT-9921 and the VoidLink framework in this campaign may signal an incremental evolution in threat tradecraft. VoidLink's reconnaissance and potential lateral-movement capabilities could introduce added exposure for technology and financial services organizations, particularly in cloud-heavy environments.

Technical Details

- UAT-9921 has been active since at least 2019, using compromised hosts to deploy VoidLink C2 for reconnaissance.
- The VoidLink framework is modular and specifically targets Linux systems, with indications of Windows compatibility.
- Operators have access to the source code of VoidLink modules, indicating a deep understanding of the framework.
- Compromise methods include the use of pre-obtained credentials and exploiting Java serialization vulnerabilities.
- Initial compromise may occur via malicious documents, although no samples have been confirmed.

- UAT-9921 deploys a SOCKS server on compromised servers to facilitate internal scanning and lateral movement.
- The framework supports compilation on demand for plugins, enhancing its adaptability across different Linux distributions.
- VoidLink features advanced stealth mechanisms to evade detection, including anti-forensics and evasion strategies against EDR solutions.
- The framework includes role-based access control (RBAC) for operational oversight, which is uncommon in similar frameworks.
- VoidLink's rapid development cycle, aided by AI-enabled IDEs, indicates a significant evolution in attack frameworks.

Recommendations

- Implement network segmentation to limit lateral movement opportunities for potential intruders.
- Regularly update and patch systems to mitigate vulnerabilities, particularly those related to Java serialization.
- Monitor for unusual outbound traffic patterns indicative of C2 communication.
- Employ advanced endpoint detection and response (EDR) solutions to identify and mitigate stealthy threats.
- Conduct regular security awareness training for employees to recognize and avoid potential phishing attempts.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
New XWorm Campaign Utilizing Multiple-Themed Phishing Emails	HIGH	CLEAR	Campaign	Open Source

Executive Summary

FortiGuard Labs recently identified a phishing campaign delivering the XWorm Remote Access Trojan (RAT) through malicious Excel attachments. This multi-stage attack utilizes social engineering tactics to persuade Windows users to open infected files, leading to full remote control of their systems.

This campaign appears to leverage known vulnerabilities (e.g., CVE-2018-0802) alongside XWorm RAT functionality, which could increase exposure for financial services organizations, particularly where patching and controls are not fully applied.

Technical Details

- The campaign begins with phishing emails that deliver malicious, business-themed Excel attachments engineered to exploit the CVE-2018-0802 vulnerability.

- These tailored lures are crafted to appear legitimate, increasing the likelihood that recipients will open the embedded Excel files.
- When the attachment is opened, the exploit triggers the Microsoft Equation Editor to execute embedded shellcode, which then downloads and runs the next-stage payloads.
- The shellcode downloads an HTA file that executes JScript and PowerShell code to facilitate the attack.
- A fileless .NET module is loaded into memory, utilizing process hollowing to deploy the XWorm payload within a Msbuild[.]exe process.
- The XWorm RAT establishes encrypted communication with its command-and-control (C2) server, using AES encryption for data packets.
- The XWorm payload remains in memory, avoiding detection by traditional file-based security measures.
- The malware supports a wide range of control commands, allowing attackers to manipulate victim systems extensively.
- XWorm's plugin architecture enables the addition of new features and capabilities, enhancing its threat potential.

Recommendations

- Implement advanced email filtering solutions to detect and block phishing attempts.
- Regularly update and patch systems to mitigate vulnerabilities like CVE-2018-0802.
- Conduct employee training on recognizing phishing tactics and suspicious attachments.
- Utilize endpoint detection and response (EDR) solutions to monitor for unusual process behavior.
- Establish a robust incident response plan to address potential breaches swiftly.

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
Cybercriminals Exploit Google Groups to Distribute Lumma Info-Stealer and Ninja Browser Malware	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

CTM360 has identified a global malware campaign where cybercriminals are leveraging Google Groups and Google Discussions to distribute malware. Attackers embed malicious download links disguised as legitimate software updates, tricking users into downloading malware that can exfiltrate sensitive

information. This tactic highlights the increasing sophistication of social engineering within trusted online communities, posing significant risks to both individuals and organizations.

The financial services sector may be exposed to these attack types, where malware could enable credential theft, unauthorized transactions, and data access. The use of social engineering on trusted platforms (e.g., Google) may increase user interaction rates, suggesting a need for continued vigilance and proportionate controls.

Technical Details

- Cybercriminals are leveraging Google Groups and various file-hosting services to spread malware, with researchers uncovering more than 4,000 malicious groups involved in these operations.
- Attackers embed malicious links in discussions using relevant keywords to increase credibility and lure victims.
- Malicious redirectors detect the victim's operating system (Windows or Linux) to deliver specific malware types.
- For Windows users, Lumma Info-Stealer is deployed, which exfiltrates credentials from compromised devices.
- For Linux users, a malicious browser masquerading as a legitimate tool is downloaded, enabling future compromises.
- Adversaries use shortened links and hijacked trusted domains to bypass detection.
- The malware installs scheduled tasks to maintain persistence and periodically check for updates from the threat actor's server.
- The "Ninja Browser" mimics legitimate software but contains malicious extensions that harvest sensitive information.
- Both malware types can lead to significant financial fraud and unauthorized access to sensitive accounts.

Recommendations

- Implement strict email filtering to block suspicious communications and links from Google Groups.
- Educate employees about the risks of social engineering and the importance of verifying sources before downloading software.
- Utilize endpoint detection and response (EDR) solutions to monitor for unusual activities and malware behavior.
- Enforce multi-factor authentication (MFA) for access to sensitive systems and accounts.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by malware.

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
Lazarus Group's "Graphalgo" Campaign Targets Crypto Developers with RAT	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at ReversingLabs have uncovered a new variant of the fake recruiter campaign known as “graphalgo,” linked to the Lazarus Group and aimed at targeting crypto developers. This campaign employs social engineering tactics to lure JavaScript and Python developers through fake job offers, utilizing malicious packages hosted on public repositories like npm and PyPI to deliver a Remote Access Trojan (RAT).

The impact of this campaign stems from its advanced design and modular structure, which enables the threat actor to continue operating even if specific parts of their setup are uncovered or taken down. Financial services organizations, particularly those involved in cryptocurrency and blockchain, should be vigilant as the campaign exploits trust in job recruitment to deliver malicious payloads, posing a risk to sensitive financial data and operations.

Technical Details

- The "graphalgo" campaign uses fake job offers to attract developers, with a focus on cryptocurrency-related roles.
- The campaign features a fake company, "veltrix-capital," which has a basic website and GitHub presence to lend credibility.
- Malicious functionality is introduced through dependencies in job-related repositories, obscuring the attack vector.
- The final payload is a RAT that communicates with a command and control (C2) server, supporting commands like file uploads and downloads.
- The RAT checks for the presence of the Metamask browser extension, indicating a focus on cryptocurrency assets.
- The campaign employs token-protected C2 communication, a tactic previously observed in North Korean state-sponsored operations.
- Multiple programming languages are used for the RAT payload, including JavaScript, Python, and VBS.
- The modular nature of the campaign allows for easy adaptation and continued operation despite potential exposure.

Recommendations

- Monitor and restrict the use of third-party packages in development environments, especially from public repositories.
- Educate developers about the risks associated with downloading and executing code from unverified sources.
- Employ endpoint detection and response (EDR) solutions to identify and mitigate suspicious activities related to RATs.

- Regularly review and update security protocols to address emerging threats, particularly those targeting the cryptocurrency sector.

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 Attack Campaign Utilizing ClickFix Technique Targets Users with Custom DNS Lookups	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Microsoft Defender researchers observed attackers employing the new variant of ClickFix technique, which involves social engineering tactics to trick users into executing commands that lead to malicious payloads. The latest variant utilizes a DNS-based approach, allowing attackers to deliver second-stage payloads through custom DNS lookups, enhancing evasion tactics against traditional defenses.

This campaign may introduce risk for financial services by combining social engineering with DNS-level techniques that could help bypass certain controls. The use of lightweight staging channels might blend activity into normal traffic, suggesting detection could be more challenging and warrant proportionate monitoring.

Technical Details

- Attackers use a command that performs a DNS lookup against a hard-coded external DNS server, avoiding the system's default resolver.
- The output from the DNS response is filtered to extract the Name: field, which is then executed as a second-stage payload.
- This technique enables attackers to reach their infrastructure while reducing reliance on traditional web requests.
- The attack chain includes downloading a malicious ZIP file containing a Python bundle and executing a harmful Python script for reconnaissance.
- The final payload, a remote access trojan named ModeloRAT, is dropped into the user's AppData and Startup directories for persistence.
- Microsoft Defender detects malicious activities throughout the ClickFix attack chain, blocking second-stage executions.
- The campaign uses social engineering tactics, often through phishing or deceptive prompts to trick users into executing commands.
- The attack can result in data exfiltration and deployment of follow-on malware payloads.

Recommendations

- Enhance user training programs to recognize social engineering tactics and phishing attempts.
- Implement robust endpoint protection solutions capable of detecting and blocking malicious payloads.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited in such campaigns.
- Monitor DNS queries for unusual patterns or requests to detect potential malicious activity.
- Establish incident response protocols to quickly address any signs of compromise.

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
Phorpiex Phishing Campaign Delivers GLOBAL GROUP Ransomware	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Forcepoint have identified a large-scale phishing campaign leveraging the Phorpiex botnet to distribute GLOBAL GROUP ransomware. The campaign employs phishing emails with deceptive subject lines and weaponized Windows Shortcut (.lnk) files that execute malicious payloads upon interaction. This method highlights the continued exploitation of common file types to facilitate initial system access.

The campaign's ransomware component may operate in a local-only ("mute") mode without external communication, which could reduce common detection signals. This design may complicate identification and response, suggesting that financial institutions consider proportionate enhancements to endpoint monitoring and containment capabilities.

Technical Details

- The phishing emails utilize the subject line "Your Document," which has been common in previous campaigns.
- The malicious attachment is a Windows Shortcut file disguised as a document, using double extensions to mislead users.
- Upon execution, the .lnk file launches cmd[.]exe, which in turn invokes PowerShell to download the ransomware payload.
- The payload is saved as windrv[.]exe in a system-like directory to avoid detection.
- GLOBAL GROUP ransomware operates in a fully local mode, generating its encryption keys on the compromised system.

- It does not communicate with a command-and-control server, making detection through network monitoring challenging.
- The ransomware employs anti-analysis techniques to evade detection by checking for virtualized environments and common analysis tools.
- It establishes persistence by creating a Windows service and scheduled task that executes at system startup.
- Encrypted files are marked with a unique identifier, and the ransomware appends the extension ".Reco" to encrypted files.
- The ransom note is embedded within the binary and instructs victims to contact the attackers via a Tor-based site.

Recommendations

- Implement advanced email filtering to block phishing attempts and malicious attachments.
- Educate employees about the risks of phishing and the importance of scrutinizing email attachments.
- Employ endpoint detection and response (EDR) solutions to monitor for suspicious file behaviors.
- Regularly update and patch systems to mitigate vulnerabilities that could be exploited by ransomware.
- Develop and test incident response plans to ensure quick recovery from ransomware attacks.

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
Active Exploitation of Zero-Day Vulnerability CVE-2026-2441 in Google Chrome	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Google has released an emergency security update for Chrome to address CVE-2026-2441, a use-after-free vulnerability in the CSS rendering engine. This vulnerability is being actively exploited in the wild, posing significant risks to users who visit malicious websites.

The financial services sector should be particularly vigilant, as the exploitation of this vulnerability could lead to unauthorized access to sensitive information, impacting both institutions and their clients. Immediate action is necessary to mitigate potential risks associated with this vulnerability.

Technical Details

- CVE-2026-2441 is a use-after-free vulnerability that can lead to memory corruption within the Chrome browser.

- The CVSS severity score for this vulnerability is classified as high, indicating a significant risk.
- The attack vector is remote, meaning it can be exploited through malicious web content without requiring user interaction beyond visiting a compromised site.
- No privileges are required for an attacker to exploit this vulnerability, making it accessible to a wide range of threat actors.
- The vulnerability has been confirmed as actively exploited in the wild, indicating an urgent need for remediation.
- Users must visit a malicious website for the exploit to be successful, highlighting the importance of safe browsing practices.
- The use-after-free nature of the vulnerability suggests that it could be leveraged for various types of attacks, including remote code execution.

Recommendations

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

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerability in Apple Products Allows Arbitrary Code Execution	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Apple has released critical security updates addressing multiple high-severity vulnerabilities across its entire product ecosystem, including iOS, iPadOS, macOS, and more. Among these is a zero-day vulnerability (CVE-2026-20700) that has been actively exploited in sophisticated targeted attacks, posing a significant risk to users of affected versions of iOS.

This vulnerability may introduce risk to financial services environments by enabling arbitrary code execution with memory-write capabilities. Successful exploitation could allow unauthorized access to sensitive data, suggesting that organizations consider prioritizing timely updates and proportionate control reviews.

Technical Details

- Apple has patched a critical zero-day vulnerability (CVE-2026-20700) that allows arbitrary code execution.
- The vulnerability is associated with the dyld component and has been exploited in targeted attacks against specific individuals.
- The severity of the vulnerability is classified as critical, indicating a high risk of exploitation.
- Attackers with memory write capabilities may exploit this flaw to execute arbitrary code on affected devices.

- Apple has reported that this issue may have been exploited in sophisticated attacks on versions of iOS prior to iOS 26.
- The vulnerability was addressed through improved state management to prevent memory corruption.
- Other related vulnerabilities include CVE-2025-14174 and CVE-2025-43529.
- The updates also address multiple sandbox escape vulnerabilities and kernel-level privilege escalation issues.

Recommendations

- Apply the latest security updates across all Apple devices to mitigate the risks associated with these vulnerabilities.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Code Execution Vulnerability in React Native Community CLI Actively Exploited	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical Remote Code Execution (RCE) vulnerability, tracked as CVE-2025-11953, has been identified in the @react-native-community/cli-server-api package, affecting the React Native Community CLI ecosystem. This flaw allows unauthenticated remote attackers to execute arbitrary operating system commands on developer machines running the React Native Metro development server, particularly when exposed to external networks.

This vulnerability may introduce risk to the financial services sector by enabling unauthorized access and potential control over development environments, which could affect applications and sensitive data. Organizations using React Native might consider prioritizing timely updates and proportionate control reviews to reduce exposure.

Technical Details

- CVE-2025-11953 is a critical RCE vulnerability with a CVSS v3.1 score of 9.8.
- The vulnerability allows unauthenticated remote attackers to execute arbitrary commands on affected systems.
- It impacts the @react-native-community/cli-server-api package, a core component of the React Native ecosystem.
- Specific versions affected include CLI v4.8.0 to v20.0.0-alpha.2, primarily in React Native v0.80 and v0.81.
- Active exploitation of this vulnerability has been reported, indicating an urgent need for remediation.

- The vulnerability can be exploited without local access if the development server is exposed to external networks.
- Organizations using vulnerable versions are at high risk of unauthorized command execution.

Recommendations

- Organizations should immediately apply vendor patches to address the vulnerability.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft February 2026 Patch Tuesday Security Update Addresses Multiple Critical Vulnerabilities	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Microsoft has released its February 2026 Patch Tuesday security update, addressing sixty-one vulnerabilities across its product ecosystem, including six zero-day vulnerabilities that are actively being exploited. These vulnerabilities affect various products, including Windows Desktop Manager, Remote Desktop Services, and Microsoft Office, posing significant risks to organizations using these platforms.

Reports of actively exploited zero-day vulnerabilities may warrant prioritization of remediation across financial services and other sectors. Because some issues could enable SYSTEM-level access or bypass certain security features, timely updates and proportionate control reviews may help reduce exposure.

Technical Details

- Six zero-day vulnerabilities are currently being exploited in the wild, necessitating immediate attention.
- Critical-severity vulnerabilities include privilege escalation flaws that could allow attackers to gain SYSTEM-level access.
- Affected products include Windows Desktop Manager, Remote Desktop Services, Azure services, Microsoft Office, and core Windows components.
- The vulnerabilities include CVE-2026-21519, which allows authenticated attackers to gain SYSTEM privileges via a type confusion flaw.
- CVE-2026-21533 involves improper privilege management in Windows Remote Desktop Services, enabling SYSTEM-level access.
- CVE-2026-21510 allows for a security feature bypass in Windows Shell through malicious links or shortcuts.
- CVE-2026-21514 enables attackers to bypass Protected View in Microsoft Word through malicious Office files.

- CVE-2026-21525 results in a denial of service affecting VPN/dial-up services due to a null pointer dereference.
- CVE-2026-21513 allows bypassing security features when rendering HTML in Windows applications.

Recommendations

- Prioritize remediation of the identified zero-day vulnerabilities to prevent exploitation.
- Deploy the February 2026 cumulative updates across all affected products immediately.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities in Ivanti Endpoint Manager Expose Sensitive Data	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Ivanti has released a security update addressing multiple vulnerabilities in Ivanti Endpoint Manager, which could allow remote attackers to compromise systems and exfiltrate sensitive data. The most critical vulnerability, CVE-2026-1603, permits unauthenticated attackers to bypass authentication and leak stored credential data, while another vulnerability, CVE-2026-1602, allows authenticated attackers to execute SQL injection attacks to read arbitrary database information.

Vulnerabilities in Ivanti Endpoint Manager may increase exposure for financial services and adjacent sectors that rely on the platform, potentially enabling unauthorized access and data exfiltration. Timely updates and proportionate control reviews could help reduce risk to sensitive information.

Technical Details

- Ivanti has disclosed two vulnerabilities in Ivanti Endpoint Manager, one rated HIGH and one rated MEDIUM.
- The most severe vulnerability, CVE-2026-1603, allows unauthenticated attackers to bypass authentication and access stored credentials.
- CVE-2026-1602 enables authenticated attackers to perform SQL injection attacks, potentially leading to unauthorized data access.
- The vulnerabilities affect Ivanti Endpoint Manager versions 2024 SU4 SR1 and all prior versions.
- A total of eleven additional medium severity vulnerabilities from October 2025 have also been resolved in this update.
- The vulnerabilities could lead to significant data breaches if exploited by malicious actors.

Recommendations

- Apply the latest security updates (version 2024 SU5) to Ivanti Endpoint Manager immediately.

- Prioritize patching for internet-facing or publicly accessible installations of the software.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities Identified in Fortinet Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Fortinet has disclosed several vulnerabilities affecting its products, including critical flaws in FortiClientEMS, FortiOS, and FortiSandbox. These vulnerabilities could allow unauthenticated remote attackers to execute unauthorized commands or bypass authentication mechanisms, posing significant risks to affected systems.

Vulnerabilities affecting Fortinet products may increase exposure for financial services by enabling unauthorized access and potential data exploitation. Timely remediation and proportionate control reviews could help reduce risk to sensitive systems and information.

Technical Details

- CVE-2026-21643: A critical vulnerability in FortiClientEMS due to insufficient input validation, allowing remote attackers to execute unauthorized commands via crafted HTTP requests.
- CVSS v3 Score: 9.1 indicates a critical severity level for CVE-2026-21643, emphasizing the urgency for remediation.
- CVE-2026-22153: An authentication bypass vulnerability in FortiOS that may allow unauthenticated attackers to bypass LDAP authentication under specific configurations.
- CVSS v3 Score: 7.5 for CVE-2026-22153, categorized as high severity, necessitating immediate attention.
- CVE-2025-52436: A cross-site scripting vulnerability in FortiSandbox, enabling unauthenticated attackers to execute arbitrary commands through crafted HTTP requests.

Recommendations

- Update all affected Fortinet products to the latest patched versions to mitigate identified vulnerabilities.

Detailed Vulnerability Details and Affected Products can be found at *link1*, *link2*, *and link3*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Figure Technology Suffers Data Breach Exposing Customer Information	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

Figure Technology, a blockchain-based lending company, has confirmed a data breach resulting from a social engineering attack that compromised a limited number of files. The breach was attributed to the hacking group ShinyHunters, which claimed responsibility and published a significant amount of allegedly stolen data.

This incident appears relevant to financial services sector, as it highlights both the risks of social engineering and the exposure that can arise from relying on third-party identity providers like Okta. Since Okta manages critical authentication processes, any compromise of its support workflows or administrative controls can cascade into downstream environments, leading to unintended disclosure of customer details such as names, addresses, and contact information. The event underscores the need for stronger verification steps within Okta's support processes, more robust oversight of identity vendors, and tighter data-handling and authentication controls across fintech operations to reduce the impact of similar threats.

Technical Details

- The breach was initiated through a social engineering attack targeting an employee of Figure Technology.
- Hackers managed to steal a limited number of files containing sensitive customer information.
- ShinyHunters, the responsible hacking group, published 2.5 gigabytes of allegedly stolen data on their dark web leak site.
- The leaked data included customers' full names, home addresses, dates of birth, and phone numbers.
- The attack is part of a broader campaign targeting customers using the single sign-on provider Okta.
- The breach emphasizes the ongoing threat posed by social engineering tactics in cyberattacks.

Recommendations

- Implement robust employee training programs focused on recognizing and responding to social engineering attacks.
- Enhance security measures around third-party authentication providers to mitigate risks.
- Regularly review and update incident response plans to address potential breaches effectively.
- Offer identity theft protection services to customers as a proactive measure.
- Monitor for unusual account activity and implement multi-factor authentication for added security.

Reference to the Source

back to top

Appendix A – 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 B – 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 C - Acronyms & Technical Terms

Term / Acronym	Meaning / Description
AES (encryption)	Algorithm used by XWorm to encrypt traffic with its command-and-control server.
AppData / Startup (Windows)	Common Windows directories abused to maintain persistence for malware.
Apple devices (iOS, iPadOS, macOS)	Platforms patched for a zero-day (CVE-2026-20700) enabling arbitrary code execution.
Azure services	Part of the Microsoft ecosystem listed among affected products in the February update set.
C2 (Command and Control)	Attacker-operated systems that send instructions to compromised machines and receive stolen data.
CHROMEPUSH	Malicious browser extension that captures keystrokes and browser cookies from victims.
ClickFix	Prompt-based technique that convinces users to run commands; latest variant stages payloads using custom DNS lookups.

cmd.exe / PowerShell chain	Command sequence launched by .lnk files to retrieve and execute ransomware binaries.
Cross-site scripting (XSS)	Web flaw that allows attacker-supplied scripts to run in a user's browser.
Cryptocurrency / DeFi (decentralized finance) exposure	Areas noted as at higher risk from campaigns focused on crypto assets and related firms.
CSC	UAE Cyber Security Council
Custom DNS lookup	Request to a specific external DNS server whose response encodes the next command to execute.
CVE-2018-0802 (Equation Editor)	Legacy Microsoft Equation Editor flaw exploited by booby-trapped Excel files to run code.
CVE-2025-11953	Critical remote code execution issue in @react-native-community/cli-server-api affecting Metro dev servers if exposed.
CVE-2026-1602	Ivanti SQL injection vulnerability allowing reading of arbitrary database information by authenticated users.
CVE-2026-1603	Ivanti flaw allowing unauthenticated access to stored credential data.
CVE-2026-20700	Apple zero-day in the dyld component that enables arbitrary code execution on affected devices.
CVE-2026-21510 / CVE-2026-21514 / CVE-2026-21513 / CVE-2026-21525	Microsoft issues including security feature bypass, Protected View bypass, HTML rendering bypass, and denial of service.
CVE-2026-21519 / CVE-2026-21533	Examples of Microsoft flaws enabling SYSTEM-level privileges or other high-impact outcomes.
CVE-2026-2441	Actively exploited Google Chrome use-after-free flaw in the CSS rendering engine that requires urgent updating.
CVSS	Standard severity scoring system referenced to communicate vulnerability risk.
DEEPBREATH	Malware that tampers with macOS privacy settings (TCC database) to access sensitive data without approval.
Deepfake video	AI-generated video used to impersonate a real person to gain trust and convince targets to run harmful actions.
Developer toolchain risk	Threats targeting build/test systems and public packages that can compromise software and data.
DNS-based staging / Unusual DNS activity	Use of DNS lookups and responses to deliver or encode payloads, which can blend into normal traffic.
Double extensions	Deceptive file naming trick that makes executable shortcuts appear to be harmless documents.
dyld	Apple dynamic loader component implicated in the cited arbitrary code execution issue.
EDR (Endpoint Detection and Response)	Security tooling used to detect, investigate, and contain malicious activity on devices.
Figure Technology breach	Fintech incident triggered by social engineering that exposed customer data such as names and contact details.
Fileless .NET module	Malicious component that runs only in memory to avoid traditional file-based detection.
FortiClientEMS	Fortinet product with a critical command execution flaw due to insufficient input validation (CVE-2026-21643).
FortiOS	Fortinet operating system affected by an LDAP authentication bypass under certain configurations (CVE-2026-22153).
FortiSandbox	Fortinet analysis product with a cross-site scripting (XSS) issue (CVE-2025-52436).
GLOBAL GROUP ransomware	Ransomware that can encrypt files locally without contacting external servers, reducing network alerts.
Google Chrome (browser)	Product affected by an actively exploited CSS rendering engine vulnerability (CVE-2026-2441).
Google Groups / Google Discussions abuse	Use of trusted Google forums to embed links that install info-stealers or rogue software.

graphalgo (campaign)	Recruiter-themed effort attributed to Lazarus that delivers a RAT via poisoned npm and PyPI packages.
HTA / JScript / PowerShell	Scripting components used after exploitation to fetch and execute follow-on payloads.
HYPERCALL	Downloader component that retrieves further malware from attacker infrastructure.
Ivanti Endpoint Manager	Enterprise platform affected by an authentication bypass leaking stored credentials and an SQL injection issue.
Java serialization vulnerability	Software flaw referenced as a path to initial access or code execution by UAT-9921.
Lateral movement	Spreading from one compromised system to others within the same environment.
Launch daemons (macOS)	Auto-start mechanism on macOS abused to keep malware persistent after reboot.
Lazarus Group	Campaign targeting crypto developers with fake job offers and malicious packages hosted on public repos.
LDAP	Directory-based sign-in method implicated in the FortiOS authentication bypass scenario.
Local-only “mute” mode	Ransomware behavior where key generation and encryption happen on the victim system without C2 traffic.
Lumma Info-Stealer	Malware that extracts credentials and other sensitive information from Windows devices.
Metamask (extension)	Browser wallet extension whose presence is checked by the Lazarus RAT, indicating a crypto focus.
MFA (Multi-Factor Authentication)	Additional verification steps recommended to reduce unauthorized access.
Microsoft February 2026 updates	Monthly fixes that include several actively exploited issues across Windows and Office.
Microsoft Patch Tuesday (Feb 2026)	Update cycle that fixed 61 issues, including six zero-days across Windows and Office components.
ModeloRAT	Remote access trojan delivered by the ClickFix chain and set to persist in user profile locations.
Msbuild.exe	Legitimate Windows process abused as a host process for the XWorm payload.
Ninja Browser	Malicious Linux browser that mimics a legitimate tool and includes harmful extensions to harvest data.
npm / PyPI	Public software package repositories leveraged to deliver malicious dependencies into developer environments.
Null pointer dereference	Programming fault that can crash services or cause denial of service in VPN/dial-up components.
Okta	Single sign-on provider referenced as part of the broader campaign tied to the breach context.
Phishing	Fraudulent messages that lure recipients into opening malicious files or links, often disguised as business documents or updates.
Phorpiex	Botnet used to send high-volume phishing that installs GLOBAL GROUP ransomware via weaponized shortcuts.
Process hollowing	Technique that injects malicious code into a benign process (e.g., Msbuild.exe) to hide activity.
Protected View (Office)	Office safeguard that one vulnerability allowed attackers to bypass using malicious files.
RAT (Remote Access Trojan)	Malware that provides remote control of an infected device, enabling commands and data theft.
RBAC (Role-Based Access Control)	Access controls built into VoidLink operations to govern what different operator roles can do.
RCE (Remote Code Execution)	A flaw that lets an attacker run arbitrary commands on a target system.

React Native Metro development server	Developer server that, if reachable from external networks, can allow commands to run on developer machines.
Reconnaissance (internal/external)	Information-gathering to map systems and services before further attack actions.
Sandbox escape / Kernel privilege escalation	Apple vulnerability types addressed that break isolation or grant elevated system rights.
Scheduled tasks / Startup folders	Windows mechanisms used by malware to relaunch automatically and maintain persistence.
Shellcode	Low-level code executed after an exploit to download or run the next attack stage.
ShinyHunters	Hacking group that claimed responsibility for publishing the allegedly stolen Figure Technology data.
SILENCELIFT	Malware family used in UNC1069 operations as part of a larger toolkit on victim hosts.
Social engineering	Deceptive tactics (e.g., fake recruiters, deepfake video, misleading prompts) that trick people into taking actions that aid an attack.
SOCKS server	Proxy service deployed on compromised hosts to enable internal scanning and movement within a network.
SSO (Single Sign-On)	Centralized login approach mentioned in the breach context, highlighting third-party authentication risk.
TCC (macOS) database	macOS permissions store targeted to gain unauthorized access to protected data.
Telegram (compromised account)	A hijacked messaging account used as a starting point for social engineering in the UNC1069 campaign.
Token-protected C2	C2 communication that requires a token for interaction, noted in the graphalgo campaign.
Tor-based site	Anonymized website referenced in ransom notes for victim contact.
UAT-9921	Newly observed threat actor that installs VoidLink for command and control and reconnaissance, with a focus on Linux systems.
UNC1069	Financially motivated North Korean threat actor targeting cryptocurrency firms using compromised accounts, deepfakes, and multiple malware families.
URL shorteners / redirectors	Link cloaking and redirection methods used to evade detection and tailor payloads to the victim's OS.
Use-after-free	Memory error that attackers can exploit to run code, as seen in the Chrome vulnerability.
veltrix-capital	Fake company identity used to add credibility to the graphalgo recruiting approach.
VoidLink	Modular attack framework used to set up C2, scan internal networks, and manage implants with stealth features.
WAVESHAPER	Backdoor used by UNC1069 to deliver additional malicious payloads after initial compromise.
Windows Desktop Manager / Remote Desktop Services	Windows components named as affected by issues in the month's patch release.
Windows Desktop Manager / Remote Desktop Services / Windows Shell	Windows components called out as affected in the February update set.
Windows Shortcut (.lnk)	Shortcut file abused to trigger command sequences that download and run malware.
XWorm	Remote Access Trojan delivered through malicious Excel attachments, giving attackers control of victim systems.
Zero-day	A vulnerability that is actively exploited before or at the time a fix is released.
Zoom (fake meeting)	Bogus video meeting used to present a deepfake and trick victims into executing attacker-supplied commands.