TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	18/3/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 18 March 2026

9	6	0	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 Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a sustained escalation in both state-sponsored and financially motivated cyber activity, with a pronounced focus on destructive malware, credential theft, and exploitation of internet-facing infrastructure. Multiple high-confidence campaigns linked to Iranian and China-nexus threat actors demonstrate increasing sophistication, including wiper malware deployments, adversary-in-the-middle phishing, AI-assisted social engineering, and abuse of cloud and blockchain technologies. Across the reporting period, attackers leveraged edge device vulnerabilities, compromised websites, SEO manipulation, and trusted enterprise tools to bypass detection and accelerate post-compromise activity. Concurrently, several actively exploited and high-severity vulnerabilities were disclosed across widely used platforms including Microsoft, Google Chrome, Fortinet, SAP, Ivanti, and Cisco. From a financial sector perspective, these developments heighten risks to operational resilience, identity systems, cloud environments, and critical business services. Destructive attacks targeting availability, combined with rapid credential theft and privilege escalation, underscore the need for disciplined patch management, strong identity controls, continuous monitoring, and executive-level readiness for disruptive cyber incidents. Stakeholders should ensure timely remediation, validated backups, enhanced security awareness and coordinated incident response governance.

ADGM THREAT INTELLIGENCE SUMMARY

SAP Security Patch Day Addresses Critical Vulnerabilities in Enterprise Products [Vulnerability] [Medium]

Cisco Addresses Multiple Vulnerabilities in IOS XR Software and Contact Center Products [Vulnerability] [Medium]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Iranian Threat Actors Increase Use of Wiper Malware in the Region	HIGH	CLEAR	Campaign	CSC

Executive Summary

Recent intelligence indicates that Iranian-linked threat actors are escalating their use of wiper malware, a destructive cyber weapon designed to permanently erase data and incapacitate systems. This malware has been strategically deployed against various targets in the Middle East.

The implications of this campaign may impact organizations within the financial services sector, as the destructive nature of wiper malware poses risks to critical infrastructure and operational continuity. Financial institutions in the region should be aware of these threats and consider enhancing their defenses against potential destructive cyber operations.

Technical Details

- Wiper malware is engineered to erase data permanently, leaving systems inoperable and with no recovery options.
- Initial access is often gained through spear-phishing or exploiting VPN vulnerabilities to deploy malware or remote access tools (RAT).
- Discovery phase includes Active Directory reconnaissance to identify key assets and network shares.
- Privilege escalation techniques involve dumping credentials from LSASS using tools like Mimikatz and employing token impersonation.
- Lateral movement is executed via remote commands using PsExec or WMI, and techniques like pass-the-hash are used for system traversal.
- Wiper staging involves disabling security tools and deploying destructive payloads through Group Policy or drivers.
- Data destruction methods include overwriting the Master Boot Record (MBR) and critical disk structures, as well as corrupting files and partition tables.
- Multiple Iranian threat actors are involved, with over six active actors and more than eight wiper variants identified.
- Notable threat actors include VOLATILE KITTEN, BANISHED KITTEN, and PULSAR KITTEN, each linked to various wiper variants.
- The campaign is characterized by its focus on disruption rather than financial gain, underscoring its geopolitical motivations.

Recommendations

- Implement immutable offline backups following the 3-2-1 backup rule and test restoration processes monthly.
- Utilize Windows Defender Application Control (WDAC) or AppLocker to block unsigned drivers and prevent wiper malware execution.
- Enforce multi-factor authentication (MFA) for all remote access to enhance security.
- Promptly patch VPN and edge devices, especially those affected by vulnerabilities like Log4j.
- Conduct immediate hunting for indicators of compromise (IOCs) related to wiper malware activities.
- Activate and validate incident response procedures, ensuring clear escalation paths and coordination between technical teams and executive leadership during destructive cyber incidents.
- Elevate SOC monitoring and proactive threat hunting across critical systems to detect anomalous administrative behavior, unusual authentication patterns, and lateral movement.
- Review and harden privileged access controls, enforcing strict monitoring of domain administrators, service accounts, and all remote administrative access.
- Validate network segmentation and restrict unnecessary connectivity between user networks, servers, backup systems, and operational infrastructure.
- Monitor for early warning indicators such as mass file deletion, log tampering, suspicious script execution, and other abnormal system activity.

For a detailed cyber kill chain, refer to the Annexure – Iranian Threat Actors Increase Use of Wiper Malware in the Region

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Adversary-in-the-Middle Phishing Campaign Targets AWS Management Console Credentials	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Datadog Security Research has identified an active adversary-in-the-middle (AiTM) phishing campaign targeting AWS Management Console credentials. This campaign utilizes a phishing kit that proxies authentication to the legitimate AWS sign-in endpoint in real time, capturing validated credentials and potentially one-time password (OTP) codes before redirecting victims. Unauthorized access to the AWS Management Console occurred within 20 minutes of credential submission, highlighting the speed at which compromised credentials were exploited.

Organizations in the financial services sector should be aware of this campaign as it poses risks to AWS Management Console users, particularly those managing sensitive financial data. The use of typo squatted domains that mimic AWS infrastructure could lead to credential theft and unauthorized access to critical systems. Financial institutions must remain vigilant against such phishing attempts, as they may impact the security posture of their cloud environments.

Technical Details

- The phishing kit employs real-time AiTM proxying to capture credentials and session information.
- It uses typo squatted domains that closely resemble legitimate AWS infrastructure, enhancing its credibility.
- The phishing page is a high-fidelity clone of the AWS Management Console sign-in page, serving static assets that mirror the legitimate UI.
- Multi-stage redirects are used to obscure the phishing link, starting from a click-tracked AWS SES domain.
- The kit functions as a transparent reverse proxy, forwarding credentials to the legitimate AWS endpoint and relaying responses back to the victim.
- An administrative panel exposed on TCP port 3000 allows attackers to monitor captured credentials and manage active phishing URLs.
- The campaign has demonstrated rapid infrastructure rotation, with new phishing domains registered shortly after initial observations.
- Post-compromise authentication was detected from a Mullvad VPN egress node, suggesting automated credential testing or active monitoring by the attacker.
- The phishing kit may support real-time capture of two-factor authentication codes.
- The campaign remains active, with ongoing updates to infrastructure and tactics.

Recommendations

- Implement multi-factor authentication (MFA) for all AWS Management Console users to mitigate credential theft risks.
- Monitor CloudTrail logs for unusual authentication events, especially from known VPN IPs.
- Educate employees about phishing tactics and the importance of verifying email sources before clicking links.
- Regularly review and update security policies related to cloud access and credential management.
- Utilize threat intelligence feeds to stay informed about emerging phishing domains and tactics.

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
Regional Escalation Fuels China-Nexus Threat Actors Lure Operations	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Check Point Research have uncovered increased activity by the China-nexus threat actor known as 'Camaro Dragon', which is targeting entities to deploy a variant of 'PlugX' malware. This escalation follows the onset of Operation Epic Fury and reflects the actor's ability to adapt operations to geopolitical developments, leveraging regional conflicts to enhance the credibility of their lures.

The implications for the financial services sector are noteworthy, as the evolving regional tensions may lead to increased espionage-motivated targeting. Organizations aligned with government, critical infrastructure, or geopolitical affairs should be particularly vigilant, as the rapid mobilization capabilities of these actors suggest potential spillover targeting patterns across Gulf Cooperation Council (GCC) countries.

Technical Details

- The campaign is attributed to 'Camaro Dragon', a China-nexus threat actor known for espionage operations.
- The actor is observed deploying a variant of the 'PlugX' malware family against entities in the region.
- Activity intensified shortly after major geopolitical escalations, indicating operational readiness.
- The threat actor uses conflict-themed lures to enhance victim engagement and increase the plausibility of their attacks.
- The attack chain likely follows a lure-driven delivery mechanism leading to malware deployment.
- The campaign demonstrates a strategic blending of geopolitical themes with established malware delivery techniques.
- Researchers noted the actor's agility in adapting lure content in response to significant events.
- The use of payloads consistent with Chinese-origin tradecraft reinforces the actor's persistence in intelligence collection.
- The activity is part of a broader pattern of increasing Chinese-linked intrusion efforts in the Middle East.
- The campaign highlights the sustained espionage intent of the threat actor.

Recommendations

- Implement enhanced monitoring for suspicious activity aligned with known China-nexus TTPs, particularly spear-phishing or lure-based intrusion attempts.
- Strengthen endpoint detection capabilities to identify behavior resembling remote-access malware deployment or persistence mechanisms.
- Improve user awareness programs focused on geopolitical-themed phishing or social-engineering lures.

- Enforce strict network segmentation and least-privilege access controls to limit lateral movement in case of compromise.
- Conduct continuous threat-hunting activities to identify anomalous processes or communication patterns associated with advanced espionage 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
FortiGate Edge Intrusions Lead to Active Directory Compromise	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Throughout early 2026, SentinelOne's Digital Forensics & Incident Response team has identified multiple incidents where FortiGate Next-Generation Firewall appliances were compromised, allowing attackers to establish unauthorized access within targeted environments. The attackers exploited vulnerabilities in Fortinet products, enabling them to extract sensitive configuration files containing service account credentials and network topology information.

This campaign may impact organizations in the financial services sector, as the compromised appliances often connect to critical authentication infrastructures like Active Directory. Financial institutions should be aware of the potential risks associated with these vulnerabilities and ensure robust logging and monitoring practices are in place to detect unauthorized access attempts.

Technical Details

- Attackers exploited vulnerabilities CVE-2025-59718 and CVE-2025-59719, which allowed unauthenticated administrative access via crafted SSO tokens.
- Another vulnerability, CVE-2026-24858, permitted attackers to log into FortiGate devices using compromised FortiCloud accounts.
- Once inside, attackers executed the command "show full-configuration" to extract configuration files, which contained encrypted service account credentials.
- The configuration files use reversible encryption, allowing attackers to decrypt and identify service accounts.
- Attackers also scanned for open FortiGate instances, attempting access using weak credentials without needing weaponized exploits.
- In one incident, a local admin account named "support" was created, enabling the attacker to establish firewall policies for lateral movement.
- The attacker used the compromised service account to authenticate to Active Directory and join rogue workstations to the domain.

- Another incident involved the creation of an "ssl-admin" account, leading to the extraction of AD administrator credentials.
- Attackers utilized Remote Monitoring and Management tools, such as Pulseway and MeshAgent, to maintain access and control over the environment.

Recommendations

- Implement strong administrative access controls on FortiGate appliances and regularly update firmware to mitigate exploitation risks.
- Restrict management access to trusted networks and require strong MFA for all administrative operations tied to directory services.
- Utilize a Security Incident & Event Monitoring (SIEM) system to aggregate logs and detect anomalies in real-time.
- Monitor for unauthorized account creation and configuration access to identify potential breaches early.
- Conduct regular security assessments and penetration testing to identify and remediate vulnerabilities in network edge devices.

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
Iranian MOIS-Linked Actors Increasingly Leverage Cybercrime Ecosystem	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Iranian-linked actors are increasingly integrating into the cybercrime ecosystem, leveraging criminal tools and services to further state objectives. This shift indicates a move from merely using cybercrime as a cover to actively participating in it, enhancing their operational capabilities and complicating attribution efforts.

The implications of this trend may impact organizations in the financial services sector, as the use of advanced malware and tactics for criminal activities could pose risks to sensitive data and operational integrity. Financial institutions should be aware of the evolving landscape where state-sponsored actors may exploit criminal networks, potentially leading to increased cyber threats.

Technical Details

- Iranian actors, particularly those linked to the Ministry of Intelligence and Security (MOIS), are increasingly engaging with the cybercrime ecosystem for operational advantages.
- Void Manticore, also known as "Handala Hack", has been observed using commercial info stealers like Rhadamanthys in targeted phishing attacks.

- MuddyWater, another MOIS-associated actor, has been linked to several cybercrime clusters, complicating attribution, and misattributing activities.
- The Tsundere Botnet, associated with MuddyWater, utilizes Node.js and JavaScript for executing malicious code on compromised systems.
- The botnet has shown adaptability by switching to Deno for execution when Node.js is detected, indicating advanced evasion tactics.
- MuddyWater's operations have been connected to the Castle Loader malware family, which serves as a downloader in various infection chains.
- The use of shared code-signing certificates between MuddyWater and Castle Loader suggests a possible overlap in operational resources.
- Recent attacks attributed to Iranian actors, including ransomware incidents, indicate a strategic use of e-crime groups branding to obscure state involvement.
- The integration of e-crime groups' tools enhances the capabilities of MOIS-linked actors while increasing the complexity of threat analysis.

Recommendations

- Implement robust monitoring and detection systems to identify unusual network activity associated with known malware families.
- Enhance incident response protocols to quickly address potential breaches linked to criminal malware.
- Conduct regular security assessments to identify vulnerabilities that could be exploited by state-sponsored actors.
- Educate employees on recognizing phishing attempts and the risks associated with engaging with suspicious communications.
- Collaborate with threat intelligence providers to stay informed about emerging threats and tactics used by MOIS-linked actors.

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
Iranian APT MuddyWater Deploys Tsundere Botnet Using EtherHiding Technique	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers at eSentire's Threat Response Unit (TRU) have identified an open-directory web server linked to the Iranian APT MuddyWater, which has been active since at least 2017. The investigation revealed the

deployment of the Tsundere botnet, which utilizes a technique called "EtherHiding" to retrieve command-and-control (C2) servers from Ethereum blockchain smart contracts. This botnet enables arbitrary command execution on compromised machines, showcasing the evolving tactics of state-sponsored threat actors.

The implications of this campaign may impact organizations within the financial services sector, particularly those involved with blockchain and virtual assets. As the Tsundere botnet leverages sophisticated techniques to establish persistence and evade detection, organizations in the financial sector should be aware of the potential risks associated with such advanced malware and consider enhancing their security postures accordingly.

Technical Details

- MuddyWater APT employs a PowerShell script named "reset[.]ps1" to deploy the Tsundere botnet and a persistence module.
- The Tsundere botnet utilizes WebSockets and AES-256-CBC encryption to establish secure channels with C2 servers.
- C2 addresses are retrieved from Ethereum blockchain smart contracts using a technique known as "EtherHiding".
- The malware checks the victim machine's language settings to determine if it is located in CIS countries, terminating execution if so.
- Tsundere sends a request to multiple RPC providers to obtain the most frequently returned C2 address.
- The botnet collects hardware identification information from the victim machine, which is sent to the C2 server.
- The persistence module installs dependencies and creates a registry entry to ensure the botnet runs at startup.
- JavaScript obfuscation techniques are employed to conceal the botnet's payloads, indicating a sophisticated level of development.
- The malware's behavior suggests it may be a Malware-as-a-Service (MaaS) offering, potentially of Russian origin.
- Artifacts from the Tsundere botnet exhibit similarities to other APT malware, indicating shared tactics among threat actors.

Recommendations

- Organizations should block access to crypto-network RPC providers commonly used by threat actors for payload staging.
- Implement a 24/7 Managed Detection and Response (MDR) service for comprehensive threat visibility and rapid incident response.
- Utilize Next-Gen AV or Endpoint Detection and Response (EDR) solutions to detect and contain potential threats.
- Regularly review and update security policies to address vulnerabilities that may be exploited by advanced persistent threats.

- Conduct employee training on recognizing and responding to phishing attempts that may facilitate such malware infections.

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 Phishing Campaign Exploits AI Email Summarization in Microsoft Copilot	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at Permiso have identified a new phishing campaign that leverages Microsoft Copilot's email summarization feature. This campaign utilizes cross prompt injection (XPIA) to manipulate AI-generated summaries, allowing attackers to embed malicious instructions within seemingly benign emails. The result is a sophisticated phishing method that exploits the trust users place in AI-generated content, potentially leading to compromised accounts and sensitive data exfiltration.

The implications of this campaign may impact organizations within the financial services sector, as it highlights a new vector for phishing attacks that bypass traditional security measures. Financial institutions should be aware of the risks associated with AI tools and consider implementing additional safeguards to mitigate the potential for exploitation through trusted interfaces.

Technical Details

- The campaign utilizes cross prompt injection (XPIA) to influence Copilot's output, creating convincing phishing content.
- Attackers append maliciously crafted text to emails, which the AI assistant may inadvertently summarize, leading to manipulated outputs.
- Different interfaces within Microsoft 365 (e.g., Outlook, Teams) exhibit varying levels of susceptibility to XPIA, with Teams being the most compliant.
- Users often perceive AI-generated summaries as legitimate, reducing skepticism towards malicious content embedded within.
- The phishing technique can escalate to data exfiltration, as Copilot can access various Microsoft 365 resources based on user permissions.
- Attackers can craft prompts that leverage internal context, making phishing attempts more convincing.
- The presence of authoritative language in AI-generated alerts can prompt users to take immediate action without scrutiny.
- The campaign demonstrates a significant trust transfer from raw email content to AI-generated summaries, complicating detection efforts.

- Security measures like Safe Links and DLP may not adequately address the risks posed by this type of attack.
- The potential for one-click exfiltration increases if the assistant retrieves sensitive information from integrated platforms.

Recommendations

- Implement user training programs to raise awareness about AI-assisted phishing tactics and encourage skepticism towards AI-generated content.
- Enhance email filtering and scanning technologies to detect and flag suspicious content before it reaches users.
- Establish strict access controls and permissions for Microsoft 365 applications to limit the potential impact of successful phishing attempts.
- Monitor user interactions with AI tools and implement alerts for unusual activities that may indicate exploitation attempts.
- Regularly review and update security policies to address emerging threats associated with AI technologies.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Storm-2561 Campaign Uses SEO Poisoning to Distribute Fake VPN Clients for Credential Theft	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Microsoft Defender Experts have identified a credential theft campaign attributed to the threat actor Storm-2561, which employs SEO poisoning to distribute fake VPN clients. This campaign redirects users searching for legitimate VPN software to malicious ZIP files that deploy trojans masquerading as trusted applications, ultimately harvesting user credentials.

The implications of this campaign may impact organizations in the financial services sector, as attackers exploit user trust in search engine results to gain access to sensitive information. Financial institutions should be aware of the potential for credential theft and the importance of implementing robust security measures to mitigate risks associated with such campaigns.

Technical Details

- The campaign uses SEO poisoning to push malicious websites to the top of search results for VPN software queries.
- Users are redirected to malicious sites that host ZIP files containing fake VPN installers.

- The malicious ZIP files include a Microsoft Windows Installer ("MSI") that mimics legitimate VPN software.
- During installation, the MSI side-loads malicious dynamic link library ("DLL") files, enabling credential collection.
- The fake VPN client presents a user interface similar to legitimate software, prompting users for their credentials.
- The trojanized software is digitally signed with a revoked certificate from Taiyuan Lihua Near Information Technology Co., Ltd.
- The "dwmapi[.]dll" file acts as an in-memory loader, launching the "inspector[.]dll" file, which is a variant of the info stealer Hyrax.
- Stolen credentials are exfiltrated to attacker-controlled command-and-control infrastructure.
- The campaign employs a post-credential theft redirection strategy to mislead users after credential capture.
- The malware establishes persistence by adding itself to the Windows RunOnce registry key.

Recommendations

- Ensure antivirus protection is updated in real time using global threat intelligence to effectively block rapidly evolving threats.
- Run endpoint detection and response (EDR) in block mode to remediate detected threats.
- Implement network protection and web protection features in security solutions.
- Enforce multifactor authentication (MFA) across all accounts to enhance security.
- Educate employees on the risks of storing enterprise credentials in browsers or personal password vaults.

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
KongTuke Campaign Exploits Compromised WordPress Sites to Deliver modeloRAT	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers at TrendAI Managed Detection and Response (MDR) have uncovered ongoing attacks linked to the KongTuke threat group, which exploits compromised WordPress websites to deliver the Python-based modeloRAT. The attackers utilize fake CAPTCHA prompts and inject malicious JavaScript into legitimate sites, prompting users to execute PowerShell commands that initiate a multistage infection process.

Organizations in the financial services sector should be aware that this campaign may impact them, particularly if their users visit compromised websites or encounter suspicious prompts. The reliance on legitimate system tools and trusted services for execution could allow the malware to evade detection, posing potential risks to enterprise environments.

Technical Details

- The KongTuke threat group employs a technique known as ClickFix, which injects malicious JavaScript into compromised WordPress sites to lure users into executing harmful PowerShell commands.
- A newer method, dubbed CrashFix, tricks users into installing a malicious Chrome extension that prompts them to follow remediation instructions, leading to infection.
- The malware checks if the infected system is part of a corporate domain and identifies installed security tools before proceeding, indicating a focus on enterprise environments.
- The initial access vector often involves users searching for specific terms and visiting compromised sites, where they encounter fake CAPTCHA prompts.
- The injected JavaScript communicates with external servers to retrieve and execute additional malicious content, allowing remote control of the infected system.
- The malware uses legitimate Windows tools, such as PowerShell and 'finger[.]exe', to execute commands and maintain persistence while minimizing visible traces.
- Reconnaissance activities include enumerating running processes and checking for security tools to avoid detection in analyst environments.
- The malware establishes persistence through scheduled tasks, executing malicious payloads at regular intervals.
- Communication with command-and-control servers occurs via HTTP POST requests, transmitting collected data and receiving further instructions.
- The campaign demonstrates a mature operation, diversifying entry techniques while maintaining a reliable post-exploitation framework.

Recommendations

- Regularly patch and update WordPress core files, themes, and plugins to mitigate the risk of compromise.
- Enhance endpoint detection and monitoring (EDR) to alert on suspicious command-line activity and unusual outbound network connections.
- Implement strong administrative controls and disable unused plugins on web servers to reduce vulnerabilities.
- Adopt a layered defensive approach that combines technical controls with continuous user education to effectively reduce organizational risk.

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
Microsoft Security Updates Address Multiple High-Risk Vulnerabilities	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Microsoft has released its March 2026 security updates to address several vulnerabilities, including two zero-day vulnerabilities and a critical remote code execution flaw. Successful exploitation of these vulnerabilities could lead to privilege escalation, denial of service, remote code execution, or information disclosure in affected environments.

Organizations in the financial services sector should be aware that these vulnerabilities may impact their operations, as they could allow unauthorized access or disruptions in services. The critical nature of the remote code execution vulnerability particularly raises concerns for systems that rely on Microsoft products, highlighting the need for timely updates and patch management.

Technical Details

- CVE-2026-21262 is a high-severity SQL Server elevation of privilege vulnerability that allows an authorized attacker to gain SQLAdmin privileges over a network.
- CVE-2026-26127 is a high-severity denial of service vulnerability in Microsoft .NET, which can be exploited by an unauthenticated attacker to disrupt services.
- CVE-2026-21536 is a critical remote code execution vulnerability in the Microsoft Devices Pricing Program, enabling arbitrary code execution on affected systems.
- CVE-2026-26110 and CVE-2026-26113 are remote code execution vulnerabilities in Microsoft Office that can be triggered through the Preview Pane without user interaction.
- CVE-2026-26144 is an information disclosure vulnerability in Microsoft Excel that may expose sensitive data and allow for data exfiltration via Microsoft Copilot integration.
- The vulnerabilities affect commonly used applications, increasing the risk of exploitation across various sectors.
- Successful exploitation could lead to significant operational disruptions and data breaches if not addressed promptly.

Recommendations

- Immediately apply the March 2026 security updates released by Microsoft across all affected systems.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-Severity Vulnerability in Google Chrome Actively Exploited	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Google Chrome has been found to contain a high-severity vulnerability identified as CVE-2026-3910, which is actively being exploited. This vulnerability arises from an inappropriate implementation within the V8 JavaScript engine, potentially allowing attackers to execute malicious web content that disrupts browser functionality. Organizations and users are urged to update their browsers immediately to mitigate risks.

The active exploitation of this vulnerability may impact organizations in the financial services sector, particularly those relying on web-based applications and services. Financial institutions should be aware that failure to address this vulnerability could expose them to significant risks, including data breaches and unauthorized access to sensitive information.

Technical Details

- CVE-2026-3910 is classified as a high-severity vulnerability affecting Google Chrome.
- The vulnerability is linked to an inappropriate implementation within the V8 JavaScript engine, which executes JavaScript code in the browser.
- Attackers can exploit this vulnerability by crafting malicious web content that triggers unintended behavior in the browser.
- Google has confirmed that this vulnerability is actively being exploited in the wild, necessitating immediate action.
- The affected versions include the latest stable releases for Windows, macOS, and Linux.
- The vulnerability type is categorized as an inappropriate implementation, indicating flaws in the code logic.

Recommendations

- Immediately update Google Chrome to the latest 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
High-Severity Vulnerability in Ivanti Desktop and Server Management Allows Privilege Escalation	Medium	CLEAR	Vulnerability	CSC

Executive Summary

A high-severity vulnerability has been identified in Ivanti Desktop and Server Management (DSM), affecting versions 2026.1 and earlier. This vulnerability allows a locally authenticated user to escalate privileges, potentially leading to unauthorized access and modification of sensitive information on affected systems.

The implications of this vulnerability may impact organizations in the financial services sector that utilize Ivanti DSM for system management. It is crucial for these organizations to be aware of the potential risks associated with this flaw and to take appropriate action to mitigate any threats that may arise from its exploitation.

Technical Details

- The vulnerability is tracked under CVE ID CVE-2026-3483 and has a CVSS score of 7.8, indicating high severity.
- It falls under the Common Weakness Enumeration (CWE) category CWE-749, which pertains to exposed dangerous methods.
- A local authenticated attacker can exploit this vulnerability to elevate privileges on the affected system.
- Successful exploitation could lead to unauthorized access, modification of sensitive information, or disruption of system operations.
- The affected versions include Ivanti Desktop and Server Management (DSM) 2026.1 and earlier.
- The fixed version is Ivanti Desktop and Server Management (DSM) 2026.1.1 or later, which addresses this vulnerability.

Recommendations

- Update Ivanti Desktop and Server Management (DSM) to version 2026.1.1 or later 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
Multiple High-Severity Vulnerabilities Disclosed in Fortinet Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Fortinet has disclosed multiple high-severity vulnerabilities affecting several of its products, including FortiManager, FortiWeb, FortiClient Linux, and FortiSwitch AXFixed. These vulnerabilities range from local privilege escalation to buffer overflow issues that could allow unauthorized access or command execution.

The implications of these vulnerabilities may impact organizations in the financial services sector that utilize Fortinet products for network security. Financial institutions should be aware of the potential risks associated with these vulnerabilities and take appropriate measures to mitigate them.

Technical Details

- A local privilege escalation vulnerability (CVE-2026-24018) in FortiClient Linux allows unprivileged users to escalate privileges to root through improper symlink following.
- A stack-based buffer overflow vulnerability (CVE-2025-54820) in FortiManager's fgtupdates service may enable remote unauthenticated attackers to execute unauthorized commands via crafted requests.
- An improper control of interaction frequency vulnerability (CVE-2026-24017) in FortiWeb permits remote unauthenticated attackers to bypass authentication rate limits, facilitating brute-force attacks on admin logins.
- A buffer overflow vulnerability (CVE-2026-22627) in FortiSwitch AXFixed allows unauthenticated attackers on the same adjacent network to execute unauthorized code by sending crafted LLDP packets.
- The vulnerabilities have been assigned CVSS scores ranging from 7.0 to 7.7, indicating a high severity level.
- Successful exploitation of these vulnerabilities may depend on specific conditions, such as the attacker's resources and the complexity of the target passwords.
- The vulnerabilities could potentially lead to unauthorized access, data breaches, or service disruptions if exploited.

Recommendations

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

Detailed Vulnerability Details and Affected Products can be found at *Link1*, *Link2*, *Link3*, *Link4*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
SAP Security Patch Day Addresses Critical Vulnerabilities in Enterprise Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

SAP has released 15 new security notes addressing vulnerabilities across several of its enterprise products, including critical platforms like NetWeaver and Supply Chain Management. Notably, the most severe vulnerabilities include code injection and insecure deserialization issues, with CVSS scores reaching up to 9.8, allowing potential execution of malicious code and compromise SAP environment.

The presence of these vulnerabilities may impact organizations within the financial services sector that utilize SAP products for their operations. Financial institutions should be aware of the necessity to implement the recommended patches promptly to mitigate risks associated with these critical and high-severity vulnerabilities.

Technical Details

- SAP released a total of 15 security notes during its monthly patch cycle, addressing various vulnerabilities across its products.
- Two critical vulnerabilities include a code injection issue in SAP Quotation Management Insurance and an insecure deserialization vulnerability in SAP NetWeaver Enterprise Portal.
- The code injection vulnerability (CVE-2019-17571) has a CVSS score of 9.8, indicating a critical risk of malicious code execution.
- The insecure deserialization vulnerability (CVE-2026-27685) has a CVSS score of 9.1, also categorized as critical.
- A high-severity denial of service vulnerability (CVE-2026-27689) was identified in SAP Supply Chain Management, with a CVSS score of 7.7.
- Affected versions for the denial-of-service vulnerability include SCMAPO 713, 714, and S4CORE 102–104.
- The vulnerabilities could allow attackers to execute malicious code or disrupt SAP services.

Recommendations

- Prioritize patching critical and high-severity vulnerabilities as outlined in the SAP security notes.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Cisco Addresses Multiple Vulnerabilities in IOS XR Software and Contact Center Products	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Cisco has released security updates to address several vulnerabilities in Cisco IOS XR Software and Cisco Contact Center products. These vulnerabilities may allow attackers to cause denial-of-service conditions, escalate privileges, or execute cross-site scripting (XSS) attacks in affected environments.

The vulnerabilities identified could potentially impact organizations in the financial services sector that utilize Cisco's technology. Financial institutions should be aware of these vulnerabilities and consider applying the recommended mitigations to enhance their security posture.

Technical Details

- CVE-2026-20118: A vulnerability in Cisco IOS XR Software could allow specially crafted traffic to cause a denial-of-service condition on affected devices.
- CVE-2026-20074: A flaw in the Multi-Instance IS-IS feature of Cisco IOS XR Software could allow crafted protocol traffic to cause a denial-of-service condition.
- CVE-2026-20040 & CVE-2026-20046: These vulnerabilities could allow a locally authenticated user to escalate privileges through the command-line interface.
- CVE-2026-20116 & CVE-2026-20117: These vulnerabilities could allow malicious scripts to be injected into a web interface and executed in a user's browser.
- Severity ratings for the vulnerabilities range from Medium to High, indicating varying levels of risk.
- The vulnerabilities affect both IOS XR Software and Cisco Contact Center products, broadening the potential impact.

Recommendations

- Apply the security updates released by Cisco.

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

back to top

Appendix A – Attack Kill Chain

Iranian Threat Actors Increase Use of Wiper Malware in the Region

KILL CHAIN STAGE	ACTIVITY
Initial Access	Spear-phishing / BEC or VPN exploit to gain entry, deploy malware or RAT to establish initial foothold
Discovery	Perform Active Directory reconnaissance, identify network shares, domain controllers, and key assets
Privilege Escalation	Dump credentials from LSASS (e.g., Mimikatz), use token impersonation or kernel drivers to gain admin access
Lateral Movement	Execute remote commands using PsExec or WMI, use pass-the-hash or scheduled tasks to move across systems
Wiper Staging	Disable security tools such as AV/EDR, deploy destructive payloads via Group Policy or drivers
Data Destruction	Overwrite MBR/VBR and critical disk structures, corrupt files and destroy partition tables to disable systems

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
3-2-1 Backup Rule	Keep 3 copies, on 2 different media, with 1 copy offsite/immutable to ensure recoverability.
Active Directory (AD)	Microsoft enterprise identity service for authentication/authorization; a common attacker target.
AES-256-CBC	Encryption used by Tsundere for secure C2 traffic.
AiTM	Adversary-in-the-Middle: phishing that proxies the real login to capture live credentials and OTPs.
AppLocker	Windows feature to restrict which executables/scripts can run.
AWS Management Console	Amazon Web Services web interface for managing cloud resources; targeted for credential theft.
AWS SES Domain (Click-tracked)	Email link redirection used in the phishing flow to obscure malicious destinations.
BANISHED KITTEN	An Iranian-linked threat actor referenced in association with wiper variants.
Camaro Dragon	China-nexus espionage actor deploying PlugX with conflict-themed lures.
Cisco IOS XR	Cisco network operating system with multiple vulnerabilities addressed.
ClickFix	Technique injecting JavaScript to trick users into executing PowerShell commands.
CloudTrail	AWS logging service; recommended to monitor unusual authentication events.
Code Injection	Vulnerability that allows an attacker to run malicious code within an application.
Contact Center Products (Cisco)	Cisco suite affected by vulnerabilities including XSS and DoS.
CrashFix	Variant technique using a malicious Chrome extension to lead to infection.
CSC	UAE Cyber Security Council
CVE-2025-59718 / CVE-2025-59719	Fortinet vulnerabilities enabling unauthenticated admin access via crafted SSO tokens.
CVE-2026-21262	SQL Server EoP vulnerability granting SQLAdmin over network.
CVE-2026-21536	Critical RCE in Microsoft Devices Pricing Program enabling arbitrary code execution.
CVE-2026-24858	Vulnerability allowing logins to FortiGate using compromised FortiCloud accounts.
CVE-2026-26110 / CVE-2026-26113	Microsoft Office RCE via Preview Pane without user interaction.
CVE-2026-26127	.NET Denial of Service vulnerability exploitable by unauthenticated attackers.
CVE-2026-26144	Microsoft Excel information disclosure, potential Copilot-related data exposure.
CVE-2026-3483 (Ivanti DSM)	Local privilege escalation due to exposed dangerous methods (CWE-749).
CVE-2026-3910	Google Chrome high-severity V8 issue actively exploited, update immediately.
CWE-749	Weakness category: Exposed Dangerous Method or Function.
Denial of Service (DoS)	Disruption of services by exhausting resources or exploiting flaws.
Discovery (AD Reconnaissance)	Attacker activity to map assets and privileges in the environment.

DLL Side-Loading	Abusing legitimate executables to load malicious DLLs.
dwmapi.dll / inspector.dll	DLL components used as loader and info stealer in the fake VPN campaign.
EDR	Endpoint Detection & Response: Detects, investigates, and blocks endpoint threats.
EtherHiding	Technique to fetch C2 addresses from Ethereum smart contracts to evade takedowns.
Executive Readiness	Preparedness of leadership to govern and direct responses during cyber incidents.
Fake VPN Client (Trojanized)	Installer that mimics legitimate VPNs but steals credentials.
finger[.]exe	Legitimate Windows tool abused in the infection chain.
FortiClient Linux	Fortinet client with a local privilege escalation issue (CVE-2026-24018).
FortiCloud	Fortinet cloud account system: Compromise enabled FortiGate access in one case.
FortiGate	Fortinet next-generation firewall, compromised in incidents leading to AD access.
FortiManager	Fortinet management product with stack buffer overflow risk (CVE-2025-54820).
FortiSwitch AXFixed	Fortinet switch with buffer overflow via crafted LLDP packets (CVE-2026-22627).
FortiWeb	Fortinet product with rate-limit bypass enabling brute-force on admin logins (CVE-2026-24017).
GCC	Gulf Cooperation Council; referenced regarding potential regional spillover targeting.
Group Policy	Windows domain mechanism sometimes abused to push malicious payloads across systems.
HTTP POST (C2)	Method used to transmit collected data and receive instructions from C2.
Hyrax (Info stealer)	Malware variant used to collect and exfiltrate credentials.
Immutable Backups	Backups that cannot be altered or deleted, protecting against destructive attacks.
Initial Access (Spear-phishing/VPN exploits)	Common entry points used by adversaries to breach networks.
Insecure Deserialization	Vulnerability allowing code execution by deserializing untrusted data.
Iranian MOIS	Ministry of Intelligence and Security; linked to actors integrating with the cybercrime ecosystem.
IS-IS (Multi-Instance)	Routing feature in IOS XR with a DoS-related flaw via crafted protocol traffic.
Ivanti DSM	Ivanti Desktop and Server Management; contains a privilege escalation flaw.
JavaScript Obfuscation	Technique to conceal malware payloads and logic.
KongTuke	Threat group using compromised WordPress sites to deliver modeloRAT.
Lateral Movement	Techniques to move from one system to another after initial compromise.
LSASS	Local Security Authority Subsystem Service: Windows component that stores/handles credentials; often targeted for credential dumping.
MaaS	Malware-as-a-Service: malware offered commercially to other threat actors.
MBR	Master Boot Record: critical disk sector; its destruction can brick systems.
MFA	Multi-Factor Authentication: requires multiple verification steps to log in.
Microsoft 365 (Outlook/Teams)	Enterprise apps with varying susceptibility to XPIA; Teams noted as most compliant.
Microsoft Copilot (Email Summarization)	AI feature targeted to influence user trust and actions via manipulated summaries.
Microsoft Patch Tuesday (March 2026)	Monthly Microsoft security updates addressing multiple high-risk issues.
Mimikatz	A tool used by attackers to extract credentials from memory (e.g., LSASS).

modeloRAT	Python-based remote access malware delivered via KongTuke operations.
MSI	Microsoft Installer package leveraged to side-load malicious DLLs.
MuddyWater (APT)	Iranian APT linked to Tsundere botnet, Castle Loader overlaps, and broader cybercrime clusters.
Mullvad VPN (egress node)	A VPN endpoint observed as the source of post-compromise logins in the phishing campaign.
Node.js / Deno	JavaScript runtimes used by attackers; Tsundere can switch to Deno if Node.js is detected.
Pass-the-Hash	Using stolen password hashes to authenticate without knowing plaintext passwords.
PlugX	Malware family commonly associated with Chinese espionage operations.
PowerShell	Windows scripting tool abused to execute malicious commands.
Privilege Escalation	Gaining higher-level access within a system or network.
Privilege Escalation (CLI)	IOS XR flaws allowing local users to gain higher privileges.
PsExec	A Windows admin tool frequently abused for remote command execution and lateral movement.
PULSAR KITTEN	An Iranian-linked threat actor associated with wiper operations.
Reverse Proxy (Transparent)	Infrastructure that relays victim credentials to legitimate services while eavesdropping on sessions.
Revoked Certificate (Taiyuan Lihua Near Information Technology Co., Ltd.)	A revoked code-signing certificate observed on the trojanized software.
RMM Tools (Pulseway, MeshAgent)	Remote monitoring tools abused by attackers to persist and control environments.
RPC Providers (Crypto)	Blockchain access endpoints queried to resolve C2 addresses.
RunOnce Registry Key	Windows persistence mechanism leveraged by the malware.
Safe Links	Protective email feature mentioned as potentially insufficient against XPIA-based attacks.
SAP NetWeaver Enterprise Portal	SAP platform affected by insecure deserialization (critical).
SAP Quotation Management Insurance	SAP product with critical code injection issue.
SAP Security Patch Day	Monthly SAP patches addressing critical/high vulnerabilities.
Scheduled Tasks	Windows mechanism used to achieve persistence.
SEO Poisoning	Manipulating search rankings to drive victims to malicious downloads.
Service Account	Privileged non-human account; often targeted once device configs are stolen.
SIEM	Security Information & Event Management: aggregates logs and detects anomalies.
Storm-2561	Threat actor running SEO poisoning to distribute fake VPN clients for credential theft.
Token Impersonation	Abusing legitimate tokens to adopt another user's privileges.
Tsundere Botnet	MuddyWater botnet enabling arbitrary command execution and persistence.
Typo squatting	Registering lookalike domains to trick users into visiting malicious sites.
V8 JavaScript Engine	Chrome's JavaScript engine where the vulnerability resides.
Void Manticore / Handala Hack	Actor noted using commercial info stealers in targeted phishing.
VOLATILE KITTEN	An Iranian-linked threat actor noted in the wiper campaign context.
WDAC	Windows Defender Application Control: policy-based control to block untrusted code/drivers.
WebSockets	Communication channel used by Tsundere for interactive C2.
Wiper Malware	Destructive malware designed to permanently erase data and render systems inoperable.
WMI	Windows Management Instrumentation: interface attackers use for remote execution and reconnaissance.

WordPress (Compromised Sites)	Legitimate sites injected with malicious JavaScript to lure users.
XPIA	Cross Prompt Injection Attack: manipulates AI-generated summaries (e.g., Copilot) to embed malicious instructions.
XSS (Cross-Site Scripting)	Web injection where malicious scripts execute in a user's browser.