TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	15/4/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 15 April 2026

6	8	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 concentrated surge in high-severity threat activity spanning state-aligned espionage, fast-moving criminal ransomware operations, large-scale phishing, and exploitation of internet-exposed infrastructure. The entries collectively show adversaries abusing trusted platforms, edge devices, and common user workflows including browsers, email, and remote access systems to gain rapid access, persist undetected, and escalate impact. From a financial sector perspective, the newsletter underscores elevated risk to availability, confidentiality, and trust, driven by credential theft, privilege escalation, DNS manipulation, ransomware acceleration, and weaknesses in identity, VPN, and endpoint software. Stakeholders should prioritize rapid patching of exposed systems, tighter control over remote access and DNS, phishing-resistant authentication, and readiness for fast exploitation during geopolitical or vulnerability disclosure events.

ADGM THREAT INTELLIGENCE SUMMARY

Name	Threat Severity Rating	TLP	Attribution	Originating Source
APT28 Leverages Compromised SOHO Routers for DNS Hijacking and TLS AiTM Interception	HIGH	CLEAR	Campaign	CSC

Executive Summary

Researchers have identified a large-scale cyber-espionage campaign by Forest Blizzard (APT28) that compromises SOHO (Small Office/Home Office) routers, alters DHCP settings to push actor-controlled DNS resolvers, and then spoofs DNS responses for selected domains to enable adversary-in-the-middle (AiTM) interception of TLS connections, including Microsoft Outlook on the web. The activity has been observed since at least August 2025, impacting 200+ organizations and 5,000+ consumer devices globally.

This campaign may be relevant to organizations in the financial sector, particularly where remote or hybrid users rely on SOHO networks and cloud email services. This may increase the likelihood of DNS hijacking preconditions and could impact the integrity of user access to email and cloud-hosted content if DNS and TLS controls are not enforced.

Technical Details

- The actor exploited vulnerable or weakly configured SOHO routers to gain initial access at the network edge.
- After compromise, the actor modified router DHCP settings to distribute actor-controlled DNS resolver addresses to all connected endpoints.
- The campaign used *"dnsmasq"* as the DNS forwarding/caching utility on actor-controlled infrastructure, listening on port 53 for DNS queries. Legitimate DNS tooling was repurposed to blend in while enabling traffic observation and manipulation.
- In the broad phase, DNS requests were largely proxied transparently to legitimate services to keep connectivity normal.
- In the selective phase, the actor spoofed DNS responses for targeted domains (including Microsoft 365/Outlook on the web). Victims were redirected to interception infrastructure for active AiTM against intelligence-priority targets.
- The TLS proxy servers presents invalid TLS certificates, relying on users bypassing certificate warnings.
- The campaign is attributed to GRU GTsSS Military Unit 26165 (Forest Blizzard).

Recommendations

- Audit SOHO routers used by remote/hybrid staff: verify firmware status and confirm DNS/DHCP settings have not been altered, replace end-of-life devices.
- Deploy endpoint controls that force DNS resolution through trusted, organization-controlled resolvers (e.g., Zero Trust DNS), and alert on resolver changes.
- Implement comprehensive DNS logging and monitoring, baseline normal patterns, and investigate unusual resolver shifts or query volume spikes.

- Enforce strict TLS validation (prevent bypass of certificate warnings) and use certificate pinning for critical services where supported.
- Require phishing-resistant MFA and apply conditional access and sign-in risk policies to reduce the value of intercepted sessions or tokens.

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
MuddyWater State Aligned Operations Using TAG 150 CastleRAT Infrastructure	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers at JUMPSEC have identified a campaign linking MuddyWater to TAG-150's CastleRAT ecosystem by using an exposed, misconfigured command-and-control environment and a PowerShell-based deployer that installs a new *"JavaScript/Node[.]js"* agent alongside CastleRAT payloads. The activity is assessed as MuddyWater operating at least two CastleRAT builds, with additional JavaScript RAT variants deployed from the same infrastructure.

This campaign may affect financial sector organizations by using commercially available MaaS tooling alongside state-aligned targeting. This can make intrusions harder to triage, as activity may appear criminal rather than espionage-related and can complicate attribution during incident response.

Technical Details

- Analysts linked MuddyWater infrastructure to TAG-150 by analyzing a misconfigured C2 web server, multiple malware samples, and a novel PE payload. This created an evidence trail from operator-controlled infrastructure to MaaS-delivered components.
- A key artifact was a PowerShell deployer that installs *"Node[.]js"*, decrypts an embedded payload, and drops a paired JavaScript toolset. The deployed agent *"ChainShell"* is described as previously undocumented in public reporting.
- ChainShell is a *"Node[.]js" "thin shell"* that executes server-sent JavaScript at runtime rather than carrying large built-in modules. It communicates over encrypted WebSockets, returning execution results back to the operator.
- ChainShell resolves its command-and-control location from an Ethereum smart contract via multiple RPC providers.

- CastleRAT payloads are embedded in steganographic JPEG images, indicating effort to hide binaries in seemingly benign files. Two distinct builds are referenced, supporting repeated use rather than a one-off deployment.
- The investigation assesses MuddyWater as a customer of TAG-150, based on mixed-language artifacts and platform traits.
- Code-signing certificate overlap is presented as a primary link connecting known MuddyWater tooling to the MaaS delivery chain.

Recommendations

- Monitor for unusual PowerShell-driven installation of runtimes (e.g., *"Node[.]js/Deno"*) and subsequent execution of new JavaScript agents on endpoints.
- Hunt for persistence patterns (e.g., scripted task-based execution) and investigate newly created or suspicious scheduled tasks.
- Strengthen application control and script restrictions to reduce unauthorized PowerShell and JavaScript execution paths used for deployment.
- Enforce strict code-signing validation and review newly introduced signed installers/binaries that do not align with standard software inventory.
- Add detections for abnormal outbound activity consistent with blockchain-based "dead drop" resolution patterns used to locate C2 infrastructure.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – **MuddyWater State Aligned Operations Using TAG 150 CastleRAT Infrastructure**.

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
Conflict-Themed Phishing Spoofs Emergency Alerts to Drive QR-Code Credential Harvesting	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers have identified a phishing campaign that impersonates a government emergency alert and pressures recipients to act on a "SEVERE / ACTIVE" warning by scanning a QR code for supposed safety instructions. The QR code redirects victims through a human-verification step before landing on a Microsoft-themed sign-in page designed to capture credentials.

This campaign may impact organizations in the financial sector as it leverages fear, authority, and mobile-driven QR workflows to bypass normal scrutiny and prompt rapid action. Organizations in the financial sector should be aware that credential capture via widely trusted sign-in themes could affect account security and downstream access to business email and cloud resources.

Technical Details

- The lure email impersonates a government emergency alert and references civil defense-style entities to appear authoritative. It uses a prominent "SEVERE / ACTIVE" framing to create urgency and reduce verification behavior.
- The message uses fear-inducing language to push immediate compliance.
- Rather than embedding a conventional link, the campaign relies on a QR code presented as the path to "official" instructions.
- After scanning, victims are routed to a "human verification" page that mimics a standard security check.
- The verification step is presented as successfully completed, reinforcing a false sense of legitimacy.
- Victims are then redirected to a Microsoft-themed phishing page that closely resembles a familiar sign-in portal. The page is explicitly described as intended to harvest sensitive information entered by the user.
- The campaign combines current-event theming with authoritative impersonation to widen appeal and increase click/scan rates.
- The end-to-end flow is designed to move quickly from panic → scan → verification → credential capture with minimal friction.

Recommendations

- Enable and tune protections that detect and quarantine QR-code phishing and emergency-alert impersonation themes in inbound email.
- Train users to treat QR codes in emails as untrusted, especially when paired with urgent "public safety" or "take cover" language.
- Enforce MFA and monitor for unusual sign-in patterns consistent with credential entry into a spoofed "trusted" login page.
- Block or warn on unexpected human-verification pages that precede login prompts, as this is used to build false legitimacy.

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
Storm-1175 Accelerates Medusa Ransomware by Exploiting Web-Facing Vulnerabilities	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Storm-1175, a financially motivated threat actor, runs fast-moving ransomware campaigns that exploit recently disclosed vulnerabilities in internet-facing systems before patches are widely applied. After gaining access, the actor quickly steals data and deploys Medusa ransomware, often within days and sometimes within 24 hours.

This campaign may impact organizations in the financial sector as recent intrusions included finance, and the actor's speed reduces time to detect, contain, and recover once a web-facing asset is compromised. Organizations in the financial sector should be aware that fast exploitation during patch gaps could affect availability and data protection if perimeter exposure and credential controls are not tightly managed.

Technical Details

- Storm-1175 targets vulnerable, web-facing systems during the gap between vulnerability disclosure and broad patch adoption, prioritizing exposed perimeter assets.
- Initial access is followed by rapid progression from foothold to impact, with many intrusions completing in five to six days and some in about 24 hours.
- After exploitation, the actor commonly establishes persistence by creating a web shell or dropping a remote access payload on the initially compromised device. It then reinforces access by creating a new user and adding it to the local administrators group.
- For lateral movement, Storm-1175 uses a mix of built-in tools (e.g., PowerShell, remote execution utilities) and tunneling/remote access approaches to reach additional devices.
- The actor makes heavy use of legitimate remote monitoring and management (RMM) tools to blend into normal IT activity and maintain interactive access.
- Credential theft is used to expand control, including dumping credentials from memory, and enabling credential caching via registry changes.
- Before ransomware delivery, Storm-1175 tampers with security controls by changing antivirus settings and adding broad exclusions to reduce detection.
- For double-extortion, the actor collects and exfiltrates data using common file collection and synchronization utilities, then deploys Medusa broadly.

Recommendations

- Prioritize patching and isolation of internet-facing systems; where public exposure is required, place services behind WAF/reverse proxy or a perimeter network.
- Use external attack-surface visibility to continuously identify exposed assets and reduce the window of opportunity for "disclose-to-exploit" activity.

- Strengthen credential protections: enforce least privilege, enable Credential Guard where applicable, and reduce reliance on shared local admin credentials.
- Enable tamper protections and prevent unauthorized security exclusions; treat credential-theft and security-tampering alerts as high-priority pre-ransomware signals.
- Govern RMM usage (approved list + MFA) and block or investigate unapproved RMM installations; enable automated attack disruption and relevant ASR controls to slow lateral movement.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – **Storm-1175 Accelerates Medusa Ransomware by Exploiting Web-Facing Vulnerabilities.**

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
ClipBanker Malware Distributed Through Trojanized Proxifier Software	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a campaign where victims searching for "Proxifier" are led to a repository release that bundles a malicious wrapper with a legitimate installer and "activation keys," initiating a long, multi-stage infection chain. The wrapper focuses on evasion first adding security exclusions and running PowerShell in-memory via injected (.NET) components before quietly completing delivery of ClipBanker.

This campaign may impact organizations in the financial sector as ClipBanker monitors the clipboard for cryptocurrency wallet strings and swaps them during transactions, which could affect virtual-asset payment integrity. Organizations in the financial sector should be aware the campaign relies on trusted software branding and "free license" bait, making it potentially relevant to staff who use proxy tools in secured or development environments.

Technical Details

- The infection commonly begins with a web search for *"Proxifier"*, leading users to a repository whose release package contains a malicious wrapper alongside a legitimate installer and a text file offering activation key.
- The wrapper launches the real installer to reduce suspicion while continuing malicious activity in the background.

- Early in execution, the malware attempts to weaken endpoint defenses by adding exclusions for temporary-style artifacts and the execution location. It uses an injected (.NET) component and PowerShell executed in-process to avoid visible consoles and reduce on-disk artifacts.
- The chain uses small *"donor"* processes as injection targets, then stages additional (.NET) modules that act as successive injectors.
- A later PowerShell stage performs a short set of actions: expands security exclusions to include key processes, stores an encoded script in the registry, and creates a scheduled task for follow-on execution.
- Follow-on scripts are downloaded from paste-style services using multiple layers of encoding and obfuscation. The chain then pulls a very large script from a repository location.
- The large script decodes to logic that extracts shellcode and injects it into a legitimate Windows process to run the final payload.
- The final payload is ClipBanker: it continuously monitors the clipboard for strings resembling cryptocurrency wallet addresses across many networks and replaces them with attacker-controlled values.

Recommendations

- Restrict software installation to official sources and approved repositories; treat *"free license/activation key"* bundles for paid tools as high-risk.
- Monitor for rapid creation of new security exclusions and suspicious scheduled tasks that launch script interpreters for follow-on execution.
- Increase detection coverage for in-memory PowerShell execution patterns and process injection into legitimate Windows utilities used as launch targets.
- Alert on unusual registry-stored, encoded script content and chained script downloads from paste-style hosting used to stage payloads.
- For teams handling virtual assets, reinforce transaction verification practices (e.g., out-of-band address confirmation) to reduce exposure to clipboard-manipulation scenarios.

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
ComfyUI Exposure Abused to Deploy Cryptominers and Proxy Botnet via Malicious Custom Nodes	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an active campaign targeting internet exposed ComfyUI instances where attackers abuse the custom node ecosystem to achieve unauthenticated remote code execution, then automate payload delivery at scale using a purpose-built scanner. Once code execution is obtained, compromised servers are enrolled into Cryptomining and a proxy botnet, with persistence designed to survive reboots and repeated cleanup attempts.

This campaign may impact organizations in the financial sector where AI/ML workloads or GPU-backed web services are hosted in cloud environments. Organizations in the financial sector should be aware of this tradecraft which could affect cost, availability, and security monitoring fidelity by turning high-performance infrastructure into revenue-generating mining/proxy nodes under centralized control.

Technical Details

- The campaign targets unauthenticated, internet exposed ComfyUI deployments.
- A dedicated scanner continuously enumerates cloud ranges, validates ComfyUI presence, and runs in repeated cycles to sustain high-tempo exploitation.
- After identifying a target, the tooling queries exposed node metadata to find custom nodes that execute arbitrary Python. If present, it submits a crafted workflow that executes attacker-controlled code inside the ComfyUI process.
- If no exploitable node is found, the scanner checks for ComfyUI-Manager and installs a malicious node package to create an execution path.
- The install step is abused to run attacker code, then the service is restarted, and exploitation retried.
- Post-execution, the tooling attempts to reduce visibility by clearing ComfyUI prompt/history artifacts.
- The second-stage payload “ghost[.]sh” deploys cryptocurrency miners and enrolls hosts into a Hysteria v2 proxy network, managed via a web C2 dashboard.
- Evasion includes fileless execution, process masquerading, and an *“LD_PRELOAD-style”* rootkit approach on privileged installs.

Recommendations

- Remove ComfyUI from public exposure or enforce strong access controls; avoid unauthenticated deployments and restrict administrative components like ComfyUI-Manager.
- Audit installed custom nodes and workflows for unexpected “utility/monitoring” add-ons and suspicious startup behavior indicative of reinfection logic.

- Monitor GPU hosts running ComfyUI for sudden resource spikes and unexpected proxy-style network behavior consistent with mining and traffic relaying.
- Hunt for defense-evasion patterns described in the report (fileless execution, masqueraded processes, and hiding techniques) and treat them as high-priority containment triggers.

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
BlueHammer: A Windows Zero-day Local Privilege Escalation Flaw	HIGH	CLEAR	Vulnerability	Open Source

Executive Summary

A publicly leaked proof-of-concept (PoC) exploit for an unpatched Windows local privilege escalation flaw, dubbed BlueHammer, has been observed, through which local attackers can be elevated to SYSTEM or elevated administrator permissions. The PoC was released after a researcher shared it publicly and noted it may be unreliable due to bugs, while Microsoft provided a statement that it is investigating reported issues and aims to update impacted devices.

This vulnerability may affect financial sector organizations if an attacker with initial local access uses BlueHammer to escalate privileges, potentially compromising endpoint integrity. Public availability of a PoC may reduce the time needed for attackers to gain full device control while an official fix is pending.

Technical Details

- The BlueHammer issue is described as an unpatched Windows privilege escalation flaw with public exploit code, making it a zero-day due to no available update at the time.
- Researchers confirmed the exploit works and characterized it as a local privilege escalation (LPE) that combines *"TOCTOU"* (time-of-check to time-of-use) and path confusion.
- Successful exploitation can provide access to the Security Account Manager (SAM) database, which contains password hashes for local accounts.
- The researcher who published the PoC stated there are bugs that may prevent reliable operation.
- On Windows Server, the analyst noted the exploit may elevate from non-admin to elevated administrator rather than directly to SYSTEM.

Recommendations

- Reduce opportunities for local footholds by strengthening defenses against social engineering and credential-based access paths highlighted as common entry routes.

- Prioritize rapid remediation of other software vulnerabilities to limit chaining opportunities that could lead to local execution before BlueHammer is attempted.
- Monitor for suspicious activity consistent with LPE outcomes, including unexpected privilege elevation to elevated administrator or SYSTEM.
- Add focused detection and investigation for abnormal attempts to access the SAM database, as the report ties successful exploitation to SAM hash access.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Adobe Patches Actively Exploited Acrobat/Reader Prototype Pollution RCE	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Adobe has released a Priority 1 (Critical) update for Acrobat and Reader on Windows and macOS to fix CVE-2026-34621, a prototype pollution flaw exploited via a malicious PDF to trigger arbitrary code execution. The issue is confirmed as actively exploited in the wild, increasing urgency for rapid patching.

Adobe has stated this is actively exploited and may impact organizations in the financial sector as PDF-based delivery can bypass routine user workflows and could affect endpoint. Organizations in the financial sector should be aware that unpatched desktop PDF viewers may become a high-risk entry point for broader compromise.

Technical Details

- CVE-2026-34621 is a Prototype Pollution vulnerability (CWE-1321) rated Critical with CVSS 9.6.
- Successful exploitation enables arbitrary code execution, potentially leading to full system compromise.
- Exploitation is confirmed active in the wild, indicating real-world weaponization rather than theoretical risk.
- This elevates exposure for environments where Acrobat/Reader is widely deployed on user endpoints.
- The attack vector is remote, delivered through a malicious PDF that triggers the vulnerable condition when opened.
- This makes user interaction with a crafted document the key step in the exploitation path.
- Affected products include Acrobat 2024 (Classic) up to 24.001.30356, Acrobat DC (Continuous) and Acrobat Reader DC (Continuous) up to version 26.001.21367.

Recommendations

- Immediately update affected endpoints to the listed patched versions for Acrobat/Reader and Acrobat 2024 to remove exposure.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Vulnerabilities in IBM Verify Identity and Access Solutions	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

IBM has published a security bulletin stating that multiple security vulnerabilities have been addressed in IBM Verify Identity Access and IBM Security Verify Access, affecting both appliance and container deployments across specified versions. This includes issues ranging from remote attack paths (request smuggling and SSRF) to privilege escalation and buffer overflow conditions.

This vulnerability may affect financial organizations, as weaknesses in login and access systems could allow attackers to reach important applications and systems. Organizations in the financial sector should be aware these weaknesses could affect the confidentiality of access workflows and the integrity of authentication controls if affected versions remain unpatched.

Technical Details

- CVE-2026-4101: An authentication bypass can occur under certain load conditions, allowing attackers to bypass login mechanisms and gain unauthorized access. This issue is rated CVSS 8.1.
- CVE-2026-1345: An OS command injection flaw allows unauthenticated attackers to execute arbitrary commands with lower-level privileges due to improper input validation. This issue is rated CVSS 7.3.
- CVE-2026-1343: A server-side request forgery condition allows attackers to access internal authentication endpoints that are normally protected by a reverse proxy. This issue is rated CVSS 7.2.
- CVE-2026-1188: A critical buffer overflow exists in the Eclipse OMR port library related to buffer sizing and separator handling when returning processor feature names. This issue is rated CVSS 9.8.
- CVE-2026-1346: A local privilege escalation flaw allows elevation to root due to execution with unnecessary privileges in container environments. This issue is rated CVSS 9.3.
- Additional issues include execution of scripts from an untrusted control sphere (CVE-2026-1342), an open redirect (CVE-2026-2475), and cross-site scripting conditions (CVE-2025-12635 and CVE-2026-4364).

Recommendations

- Patch immediately by updating to IBM-provided fixes: download IBM Verify Identity Access v11.0.2 IF1 and IBM Security Verify Access v10.0.9.1 IF1 and apply the corresponding container downloads for containerized deployments.

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High Severity Vulnerability in SonicWall SMA1000 Series Appliances	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

SonicWall has disclosed high severity vulnerability in SMA1000 series appliances that could allow attackers to escalate privileges via SQL injection, bypass TOTP-based MFA, and enumerate SSL VPN credentials.

This vulnerability may impact organizations in the financial sector, as SonicWall SMA appliances are commonly used for remote access. Weaknesses in these systems could affect administrative controls and user authentication, potentially impacting secure remote access if the affected versions remain in use.

Technical Details

- CVE-2026-4112 (CVSS 7.2 – High): An SQL injection vulnerability caused by improper handling of special input, allowing crafted data to be processed as part of a backend SQL query.
- The attack can be performed remotely but requires prior authentication using a read-only administrator account and specially crafted request parameters.
- Successful exploitation allows a read-only administrator to escalate privileges to Primary Administrator, resulting in full administrative control of the SMA1000 appliance.

Recommendations

- Upgrade to the latest version (12.4.3-03387+ or 12.5.0-02624+).

Vulnerability and affected product details can be found *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Mozilla Releases Security Fixes for Firefox and Thunderbird	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Mozilla has published security updates addressing multiple high-impact flaws in Firefox, including memory safety issues that may be exploitable for arbitrary code execution.

This vulnerability may impact organizations in the financial sector, as browsers and email clients are widely used in daily operations. Memory corruption issues could affect endpoint integrity if exploited through normal web activity or browser-like contexts.

Technical Details

- CVE-2026-5731 addresses memory safety bugs where some issues showed evidence of memory corruption and Mozilla presumes some could be exploited to run arbitrary code with enough effort.
- CVE-2026-5732 is described as incorrect boundary conditions leading to an integer overflow in the *"Graphics: Text component"*.
- CVE-2026-5733 is described as incorrect boundary conditions in the *"Graphics: WebGPU component"*.
- CVE-2026-5734 covers additional memory safety bugs affecting Firefox ESR and Thunderbird ESR
- CVE-2026-5735 addresses memory safety bugs specifically called out for Firefox 149.0.2 and Thunderbird 149.0.2.

Recommendations

- Upgrade Firefox and Firefox ESR fleets to the fixed versions noted in Mozilla's advisories (149.0.2, ESR 115.34.1, ESR 140.9.1) as applicable.
- Upgrade Thunderbird to 149.0.2 and Thunderbird ESR to 140.9.1 to address the listed memory safety and graphics-related issues.

Vulnerability and affected product details can be found *here*, *here*, *here*, *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Meta Addresses New High-Severity Flaw in React Server Components (RSCs) Product	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Meta has addressed a high-severity Denial of Service vulnerability in React Server Components (RSCs) tracked as CVE-2026-23869, where crafted HTTP requests to Server Function endpoints can trigger excessive CPU utilization on the server.

This vulnerability may impact organizations in the financial sector as internet-facing applications using RSC Server Functions could affect service availability if targeted with high-cost request patterns. Organizations in the financial sector should be aware that CPU exhaustion conditions can disrupt customer-facing portals and internal workflows reliant on *"Next[.]js"*/RSC-backed services.

Technical Details

- CVE-2026-23869 is a DoS vulnerability (CVSS 7.5 - High) affecting React Server Components.
- The reported impact is CPU exhaustion, leading to service degradation or outage.
- The attack vector is remote, executed through crafted HTTP requests that target Server Function endpoints.
- Applications are vulnerable if they use any of the following packages: *"react-server-dom-webpack"*, *"react-server-dom-parcel"*, or *"react-server-dom-turbopack"*.

Recommendations

- Upgrade affected deployments to "Next[.]js" 15.5.15 or 16.2.3, and update React Server packages to 19.0.5 / 19.1.6 / 19.2.5.

Vulnerability and affected product details can be found *here* and *here*.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Google Chrome Fixes Critical WebML and Multiple High-Severity Browser Bugs	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Google has released Chrome Stable Channel updates for Windows, macOS, and Linux to address multiple vulnerabilities, including critical issues in WebML and several high-severity flaws across core components.

These vulnerabilities may impact organizations in the financial sector as browsers are a primary interface for web applications and employee workflows, and unpatched clients could affect availability and integrity of endpoint sessions. Financial organizations should be aware that keeping Chrome and Extended Stable versions up to date helps reduce exposure to known high- and critical-severity issues.

Technical Details

- Google shipped *"Chrome 147 Stable"* for desktop platforms and also released Extended Stable updates for desktop. The updates address multiple issues rated Critical and High severity.
- Two Critical vulnerabilities were fixed in WebML: a heap buffer overflow (CVE-2026-5858) and an integer overflow (CVE-2026-5859). These classes of bugs can lead to unexpected memory behavior and instability when triggered through browser processing.
- Multiple High severity flaws were patched across key components, including WebRTC, V8, WebAudio, Media, Skia, Blink, and ANGLE. The listed bug classes include use-after-free, type confusion, heap buffer overflow, integer overflow, and out-of-bounds read/write.
- WebRTC includes a use-after-free fix (CVE-2026-5860), while Media and Blink also include use-after-free fixes (CVE-2026-5866, CVE-2026-5872). These issues can be triggered during normal browsing and media handling flows.
- V8 fixes include use-after-free (CVE-2026-5861), type confusion (CVE-2026-5865, CVE-2026-5871), inappropriate implementation issues (CVE-2026-5862, CVE-2026-5863), and out-of-bounds read/write (CVE-2026-5873).
- Additional WebML high-severity heap buffer overflows were addressed (CVE-2026-5867, CVE-2026-5869).

Recommendations

- Update endpoints to the fixed versions listed for Chrome 147 Stable and Extended Stable where applicable.

Vulnerability and affected product details can be found *here.*

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities in Apache Tomcat	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Apache Tomcat released updates to fix multiple vulnerabilities that could expose sensitive data or weaken certificate-based authentication, including padding-oracle issues and a code change that unintentionally weakened existing *"EncryptInterceptor"* protections.

These flaws may affect financial organizations, as Tomcat is commonly used for user authentication and application sessions, weaknesses in encryption or certificate checks could impact data protection and access control. Organizations in the financial sector should be aware that timely upgrades reduce the window for data exposure and authentication control evasion.

Technical Details

- CVE-2026-29146 is a padding oracle issue in *"EncryptInterceptor"* that can allow decryption of sensitive data.
- CVE-2026-34486 is a regression flaw in the fix for CVE-2026-29146 that enables *"EncryptInterceptor"* bypass. The bypass can result in exposure of sensitive data.
- The two *"EncryptInterceptor"* issues create a sequence where encryption protections can be weakened either by allowing it to be broken in some cases or by skipping encryption checks.

Recommendations

- Upgrade Apache Tomcat to 11.0.21+, 10.1.54+, or 9.0.117+.

Vulnerability and affected product details can be found *here* and *here.*

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

MuddyWater State Aligned Operations Using TAG 150 CastleRAT Infrastructure

Tactics	Technique
Initial Access	T1566.002 Phishing: ClickFix/BatClickFix social engineering
	T1190 CVE-2024-55591, CVE-2024-23113, CVE-2026-1281 (public-facing exploitation)
Execution	T1059.001 PowerShell
	T1059.006 Python (e.g., PyArmor-obfuscated)
	T1059.007 JavaScript (e.g., Deno/Node.js)
Execution, Defense Evasion (often used in support of Privilege Escalation)	T1218.003 CMSTPLUA COM elevation (UAC bypass)
Persistence, Privilege Escalation, Defense Evasion	T1574.002 DLL side-loading (setup.exe + userenv.dll/xmllite.dll)
Defense Evasion	T1027.003 Steganography (PE in JPEG)
	T1562.001 Defender evasion via WMI exclusions
Credential Access	T1555.003 Browser credential theft (Chrome app-bound bypass)
Command and Control	T1219 HVNC hidden desktop control
	T1090.001 SOCKS5 proxy (4,096 tunnels)
	T1102.001 Ethereum smart contract dead drop resolver

Storm-1175 Accelerates Medusa Ransomware by Exploiting Web-Facing Vulnerabilities

Tactic	Techniques	Description
Initial Access	T1190 – Exploit Public-Facing Application	Storm-1175 exploits vulnerable web-facing applications
Persistence and Privilege Escalation	T1136 – Create Account; T1098 – Account Manipulation	Storm-1175 creates new user accounts under administrative groups using the net command
Credential Theft	T1003.001 – OS Credential Dumping: LSASS Memory	Storm-1175 dumps credentials from LSASS, or uses a privileged position from the Domain Controller to access NTDS.dit and SAM hive
	T1003.003 – OS Credential Dumping: NTDS	
	T1003.002 – OS Credential Dumping: Security Account Manager	
Persistence, Lateral Movement	T1219 – Remote Access Tools	Storm-1175 uses RMM tools for persistence, payload delivery, and lateral movement
Execution	T1569.002 – System Services: Service Execution	Storm-1175 delivers tools such as PsExec or leverages LOLbins like PowerShell to carry out post-compromise activity
	T1059.001 – Command and Scripting Interpreter: PowerShell	
Exfiltration	T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage	Storm-1175 uses the synch tool Rclone to steal documents
Defense Evasion	T1562.001 – Impair Defenses: Disable or Modify Tools	Storm-1175 disables Windows Defender
Impact	T1486 – Data Encrypted for Impact	Storm-1175 deploys Medusa ransomware

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
AiTM	Adversary-in-the-Middle attack intercepting legitimate sessions
Al-Qassam	Finance-focused DDoS cyber persona associated with APT35
Apache Tomcat	Java application server widely used for web applications
APT28	State-aligned Russian cyber-espionage group also known as Forest Blizzard
APT35	Iran-aligned threat actor engaged in espionage and disruptive cyber activity
Authentication Bypass	Ability to log in without valid credentials
BellaCiao Webshell	Server-side malware enabling persistent remote access
Blockchain Dead Drop	Technique using blockchain to retrieve attacker instructions

BlueHammer	Unpatched Windows privilege escalation vulnerability
Buffer Overflow	Memory flaw leading to crashes or remote execution
CastleRAT	Commercial remote access malware used in espionage campaigns
ChainShell	JavaScript-based remote control agent deployed by MuddyWater
ClipBanker	Malware that swaps cryptocurrency wallet addresses during transactions
ComfyUI	AI image generation interface abused for server access
Command and Control (C2)	Infrastructure attackers use to manage compromised systems
CPU Exhaustion	Consumption of computing power to cause outages
Credential Harvesting	Theft of usernames and passwords via fake login pages
Cryptomining	Unauthorized use of systems to mine cryptocurrency
CSC	UAE Cyber Security Council
Custom Nodes	User-installed extensions abused to run malicious code
CVE	Common Vulnerabilities and Exposures identifier
CVSS	Scoring system ranking vulnerability severity
Denial of Service (DoS)	Attack disrupting service availability
DHCP	Network service that automatically assigns IP DNS and gateway settings to devices
DNS	Domain Name System; converts website names into network addresses
DNS Hijacking	Manipulation of DNS responses to redirect users to attacker-controlled systems
Double Extortion	Model where attackers steal data before encryption to increase pressure
EncryptInterceptor	Tomcat component responsible for encrypted session handling
Ethereum Smart Contract	Blockchain mechanism abused as a hidden command source
Firefox ESR	Long-term supported enterprise browser version
Forest Blizzard	Alternate name for APT28 linked to military intelligence activity
Geopolitical Escalation Context	Use of regional conflict themes to justify attacks
GRU GTsSS Unit 26165	Russian military intelligence unit attributed to espionage cyber operations
Human Verification Lure	Fake security step used to build trust before credential theft
Hysteria v2	High-performance proxy protocol abused for botnets

IBM Verify Identity Access	Enterprise identity and access management platform
Incident Response Playbooks	Predefined procedures for handling cyber incidents
Indicators of Compromise (IOCs)	Artifacts indicating malicious activity
Invalid TLS Certificates	Untrusted certificates used to intercept encrypted traffic
IRGC	Islamic Revolutionary Guard Corps; military organization linked to APT35
LD_PRELOAD Rootkit	Technique hijacking system execution for stealth
Local Privilege Escalation (LPE)	Attack that elevates access from user to administrator
Malicious PDF	Weaponized document used to trigger exploitation
Medusa Ransomware	Ransomware family used to encrypt systems and extort victims
Memory Corruption	Bug class allowing arbitrary code execution
Microsoft 365	Cloud productivity platform targeted via credential interception
Moses-Staff	Destructive cyber persona linked to APT35 activity
MuddyWater	Iran-aligned cyber-espionage group active against regional and corporate targets
Node[.]js	JavaScript runtime abused to run malicious agents
Outlook on the Web	Browser-based email service targeted during authentication interception
Padding Oracle	Encryption flaw allowing decryption of protected data
PowerShell	Windows scripting engine frequently abused by malware
Proof of Concept (PoC)	Public exploit showing how a vulnerability can be abused
Prototype Pollution	Flaw allowing manipulation of application logic leading to code execution
Proxy Botnet	Network of compromised systems relaying traffic
QR Code Phishing	Credential theft technique using scannable codes instead of links
Ransomware	Malware encrypting data to extort victims
React Server Components	Server-side web framework component
Remote Code Execution (RCE)	Ability to run attacker-controlled code remotely
Remote Monitoring and Management (RMM)	IT administration tools abused for persistence
Reverse Proxy	Infrastructure component protecting backend services
Sagheb RAT	Stealthy remote access trojan with credential theft capabilities

Security Account Manager (SAM)	Windows database storing password hashes
SOHO Routers	Consumer-grade routers used in small office or home office environments
SonicWall SMA	Remote access VPN appliance used in enterprises
SQL Injection	Attack manipulating backend databases
SSL VPN	Encrypted remote access channel for employees
SSRF	Attack tricking servers into accessing internal resources
Storm-1175	Threat group operating rapid ransomware campaigns
SYSTEM Privileges	Highest level of access on Windows systems
TAG-150	Malware-as-a-Service provider supplying tooling to multiple threat actors
Thunderbird ESR	Enterprise version of Mozilla email client
TLS	Encryption protocol protecting data in transit across networks
TOTP	Time-based one-time password authentication
TTPs	Tactics Techniques and Procedures used by attackers
Web-Facing Vulnerability	Weakness in internet-accessible systems
Webshell	Malicious script allowing persistent server access
WebSockets	Real-time communication channel used for covert command execution
Zero Trust DNS	Security model enforcing DNS queries through trusted services
Zero-day	A vulnerability being exploited with no official patch available