TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	12/2/2026
OVERALL THREAT SCORE	GUARDED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	UAE, MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 12 February 2026

8	5	1	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Finance Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the UAE & Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a broad range of evolving threats, including state-sponsored supply-chain compromise activity, coordinated phishing operations in the UAE, active exploitation attempts targeting development and workflow platforms, and emerging malware campaigns leveraging social engineering and browser-based lures. Several widely used technologies and products including Notepad++, React Native, n8n, ManageEngine, Chrome, Cisco products, Django, and NGINX also disclosed vulnerabilities or were observed under exploitation, suggesting an increasingly diverse attack surface across both enterprise and cloud-native environments. Additionally, cryptocurrency-focused drainer operations and a significant DeFi protocol breach illustrate how threat actors continue to adapt techniques to emerging financial technologies. For the financial sector, these developments may indicate potential exposure to unauthorized access, service disruption, and customer-facing fraud, particularly where phishing, supply-chain compromise, or vulnerable software components intersect with operational processes. Organizations could benefit from prioritizing timely patching, enhancing email and web-filter controls, reinforcing MFA, strengthening monitoring across development and automation tools, and maintaining vigilance around cryptocurrency-related interactions. Continued user awareness training and proactive configuration reviews especially for web servers, cloud services, and smart-contract integrations are likely to support improved resilience and help reduce the likelihood of downstream impact.

ADGM THREAT INTELLIGENCE SUMMARY

Targeted Supply Chain Attack Exploits Notepad++ Update Infrastructure for Malware Delivery [Campaign] [High]

Coordinated Phishing Campaign Targets UAE Using Remcos RAT via Cloud File-Sharing Abuse [Campaign] [High]

Exploitation of CVE-2025-11953 Targets React Native Development Server [Campaign] [High]

APT28 Campaign Operation Neusploit Exploits CVE-2026-21509 [Campaign] [High]

Rublevka Team Engages in Large-Scale Cryptocurrency Theft Using Sophisticated Drainer Operations [Campaign] [High]

Active Web Traffic Hijacking Campaign Targets NGINX Installations [Campaign] [Medium]

macOS Phishing Campaign Exploits AppleScript [Campaign] [Medium]

New Clickfix Variant 'CrashFix' Deploys Python Remote Access Trojan [Campaign] [Medium]

Critical Remote Command Execution Vulnerability in n8n Workflow Automation Platform [Vulnerability] [High]

High Severity SQL Injection Vulnerability in ManageEngine ADSelfService Plus [Vulnerability] [High]

Google Chrome Vulnerabilities Enabling Remote Code Execution [Vulnerability] [High]

Cisco Addresses Multiple Vulnerabilities [Vulnerability] [Medium]

Multiple Vulnerabilities Discovered in Django Framework [Vulnerability] [Medium]

CrossCurve Bridge Hacked, Resulting in $3 Million Loss [Cyber Breach] [High]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Targeted Supply Chain Attack Exploits Notepad++ Update Infrastructure for Malware Delivery	HIGH	CLEAR	Campaign	CSC

Executive Summary

Security researchers have identified a sophisticated supply-chain attack attributed to a state-sponsored APT group, which compromised the Notepad++ update service infrastructure to deliver a custom backdoor named Chrysalis. This attack did not exploit vulnerabilities in Notepad++ itself but leveraged infrastructure access to redirect update traffic to malicious payloads for selected victims.

The campaign, active from June 2025 through at least December 2025, targeted organizations aligned with specific espionage objectives, including government and critical infrastructure sectors. The use of advanced techniques highlights the ongoing risks posed by supply-chain attacks, emphasizing the need for vigilance in software update verification within the financial services sector.

Technical Details

- Attackers compromised the shared hosting server used by the Notepad++ update service, enabling them to intercept and manipulate update traffic.
- Forensic analysis revealed the server was compromised until September 2025, with credentials exposed until December 2025.
- Attackers redirected update traffic for notepad-plus-plus[.]org to their own servers, distributing malicious update manifests.
- The operation involved a multi-stage loader chain utilizing DLL sideloading and encrypted shellcode.
- The custom backdoor, named Chrysalis, was delivered alongside commodity malware tools like Metasploit and Cobalt Strike.
- The targeting was selective, consistent with state-sponsored espionage rather than widespread malware distribution.
- No vulnerabilities in Notepad++ application code was exploited, the attack exploited insufficient update verification controls.
- The campaign demonstrates an evolution in attack techniques, posing significant risks to trusted software ecosystems.

Recommendations

- Update Notepad++ immediately by manually installing version 8.9.1 or later.

- Ensure WinGup certificate and signature verification is enabled to prevent unauthorized updates.
- Conduct proactive threat hunting across endpoints and network telemetry using Indicators of Compromise (IOCs) associated with this campaign.
- Hunt for known file paths, hashes, and DLL sideloading activity to identify potential intrusions.
- Monitor for service/registry persistence artifacts and suspicious process execution chains to detect ongoing threats.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Coordinated Phishing Campaign Targets UAE Using Remcos RAT via Cloud File-Sharing Abuse	HIGH	CLEAR	Campaign	CPX-TIC

Executive Summary

CPX-TIC has identified a coordinated phishing campaign that exploits a third-party cloud-based file-sharing service (FileCloudTrial), targeting critical infrastructure entities in the UAE. The campaign utilizes sophisticated social engineering tactics, including impersonation of legitimate brands, to deliver Remcos Remote Access Trojan (RAT) malware, enabling persistent remote access to compromised systems.

The implications for the financial services sector could be significant, as this campaign demonstrates the increasing sophistication of cybercriminals leveraging legitimate cloud services to bypass traditional security measures. Financial institutions must remain vigilant against such threats, as the potential for data exfiltration and operational disruption is high.

Technical Details

- The campaign begins with a phishing email impersonating a legitimate UAE conglomerate, enticing victims to download malware.
- A malicious hyperlink redirects victims to a FileCloudTrial subdomain, increasing the likelihood of bypassing automated filters.
- Victims are prompted to download a compressed '.tar' archive containing multiple JavaScript droppers, each designed to ensure redundancy in case one is blocked.
- The JavaScript droppers are highly obfuscated, utilizing junk-code padding to evade detection by security tools.
- Upon execution, the droppers create scheduled tasks to maintain persistence across system reboots.
- The malware employs Living-off-the-Land techniques, injecting malicious code into legitimate Windows processes to evade behavioral monitoring.
- The final payload, Remcos RAT, enables extensive remote access, including keystroke logging and credential harvesting.

- The attack chain is designed to evade signature-based detection through the use of legitimate cloud services and randomized filenames.
- The identified infrastructure has been linked to a systematic pattern of targeting prominent UAE entities.
- The campaign is attributed to the Remcos RAT malware, known for its extensive remote administration capabilities.

Recommendations

- Block outbound communication on Ports 9551 and 9558 and implement a blocklist for identified C2 IP addresses.
- Enhance email filtering to flag external emails that use business-themed lures combined with external file-hosting links.
- Monitor URLs containing '*filecloudtrial[.]com' within email gateways and web proxies to prevent payload delivery.
- Configure EDR alerts to detect unusual behavior involving 'colorcpl[.]exe' and its child processes.
- Conduct regular user awareness training to improve recognition of phishing attempts targeting legitimate business services.

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

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Exploitation of CVE-2025-11953 Targets React Native Development Server	**HIGH**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

VulnCheck has observed active exploitation of CVE-2025-11953, a vulnerability in the Metro Development Server used by React Native applications. This exploitation allows unauthenticated remote attackers to execute arbitrary OS commands, indicating a significant risk to organizations utilizing this development infrastructure.

The continued operational use of this vulnerability highlights a critical gap in public awareness and response. As development tools are often inadequately monitored, the potential for exploitation poses a serious threat, necessitating immediate action to mitigate risks associated with this vulnerability.

Technical Details

- The vulnerability allows unauthenticated remote command execution via a POST request to the "/open-url" endpoint on Metro Development Server.

- Attackers utilized a multi-stage PowerShell-based loader delivered through cmd[.]exe, indicating a structured attack methodology.
- The initial PowerShell payload is base64 encoded and, when decoded, performs several actions, including adding exclusion paths for Microsoft Defender.
- The payload establishes a raw TCP connection to an attacker-controlled host, facilitating further malicious actions.
- Exploitation attempts were observed originating from specific IP addresses, indicating a coordinated attack effort.
- The payloads delivered were consistent over multiple weeks, demonstrating operational use rather than exploratory probing.
- The attackers anticipated endpoint security measures, incorporating evasion tactics into their execution flow.
- The infrastructure used for the attacks also hosted a corresponding binary for Linux, expanding the attack surface.

Recommendations

- Implement strict access controls and monitoring on development servers to limit exposure to unauthorized access.
- Regularly update and patch development tools to mitigate known vulnerabilities like CVE-2025-11953.
- Employ advanced endpoint protection solutions that can detect and respond to PowerShell-based attacks effectively.
- Conduct regular security assessments of development environments to identify and remediate potential vulnerabilities.
- Foster a culture of security awareness among developers to recognize and address risks associated with development 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
APT28 Campaign Operation Neusploit Exploits CVE-2026-21509	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Zscaler ThreatLabz has identified a new campaign, Operation Neusploit, attributed to APT28, which exploits CVE-2026-21509 using specially crafted Microsoft RTF files. This multi-stage infection chain delivers

malicious backdoors, including MiniDoor and PixyNetLoader, aimed at compromising user systems. The campaign utilizes social engineering tactics and server-side evasion techniques to target users effectively.

This campaign is notable for its sophisticated exploitation of a critical vulnerability, posing a high risk to organizations, including financial institutions. The deployment of backdoors and email stealers can lead to unauthorized access to sensitive financial data, making it imperative for organizations in the financial sector to enhance their security posture against such threats.

Technical Details

- The campaign leverages CVE-2026-21509 through crafted RTF files to initiate exploitation.
- Two variants of malicious dropper DLLs are used to deploy backdoors and steal emails.
- The first dropper, MiniDoor, is a lightweight DLL that targets Microsoft Outlook to steal emails.
- MiniDoor uses a hardcoded 1-byte XOR key for string decryption, allowing it to execute its malicious functions.
- The dropper creates a mutex and modifies registry keys to ensure malicious macros load automatically in Outlook.
- The second dropper, PixyNetLoader, employs a more complex infection chain with multiple stages.
- PixyNetLoader checks for existing files and uses COM object hijacking for persistence.
- Both droppers utilize encrypted payloads, which are decrypted and executed on the victim's system.
- The campaign employs social engineering tactics, including localized lures, to increase its effectiveness.
- Command-and-control communications are established to facilitate ongoing malicious activity.

Recommendations

- Implement robust email filtering to detect and block malicious attachments.
- Enforce multi-factor authentication (MFA) across all user accounts to mitigate unauthorized access.
- Regularly update and patch software to protect against known vulnerabilities like CVE-2026-21509.
- Conduct security awareness training for employees to recognize social engineering tactics.
- Monitor and audit registry changes and application behavior for signs of compromise.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – APT28 Campaign

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
Rublevka Team Engages in Large-Scale Cryptocurrency Theft Using Sophisticated Drainer Operations	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Insikt Group has identified a significant cybercriminal operation known as the "Rublevka Team", which specializes in large-scale cryptocurrency theft. This group has reportedly generated over $10 million through wallet draining campaigns since its inception in 2023, employing a network of social engineering specialists to direct victims to malicious pages. Unlike traditional malware approaches, Rublevka Team utilizes custom JavaScript code on spoofed landing pages that mimic legitimate crypto services, tricking victims into connecting their wallets and authorizing fraudulent transactions.

The implications for the financial services sector are profound, particularly for organizations involved in cryptocurrency transactions, fintech, and asset management. The Rublevka Team's operations pose reputational and legal risks, as customers may fall victim to these scams even outside a firm's platform. The group's ability to rotate domains and exploit RPC APIs complicates traditional fraud detection efforts, necessitating proactive monitoring and defense strategies to protect customers and maintain trust in the financial ecosystem.

Technical Details

- The Rublevka Team creates attractive offers, such as promotions or airdrops, to lure users into connecting their wallets to malicious sites.
- Their primary Telegram channel has around 7,000 members, with over 240,000 messages indicating successful wallet drains.
- Custom JavaScript drainers are embedded in landing pages, exfiltrating victims' SOL assets and compatible with over 90 wallet types.
- The group's infrastructure is automated, providing affiliates with tools for landing page creation, campaign tracking, and DDoS protection.
- Campaigns impersonate legitimate services like Phantom and Bitget to enhance user trust and conversion rates.
- The drainer utilizes various modes to manipulate wallet interactions, including "Honeypot" and "Crasher" tactics to obscure theft.
- Rublevka Team operates on multiple forums, including LolzTeam, and has shifted tactics from fake exchanges to drainer scripts.
- The group offers high commission rates to affiliates, incentivizing broader participation in their scams.
- Their operations are characterized by a high volume of transactions, with individual scams yielding profits ranging from $0.16 to over $20,000.

- The Rublevka Team's model reflects a broader trend towards scalable, service-based cybercrime in the cryptocurrency landscape.

Recommendations

- Implement robust monitoring for spoofed landing pages and phishing attempts targeting customers.
- Educate clients on recognizing legitimate crypto services and the risks of connecting wallets to unknown sites.
- Enhance fraud detection mechanisms to identify unusual transaction patterns and wallet connections.
- Collaborate with cybersecurity firms to develop takedown strategies for malicious domains associated with scams.
- Regularly update and enforce Know Your Customer (KYC) policies to mitigate risks associated with impersonation and fraud.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Cryptocurrency Theft Using Sophisticated Drainer Operations

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Active Web Traffic Hijacking Campaign Targets NGINX Installations	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Datadog Security Research has identified an active web traffic hijacking campaign that targets NGINX installations and management panels like Baota. The campaign employs malicious NGINX configurations to intercept legitimate web traffic and redirect it through attacker-controlled backend servers. This poses significant risks to organizations relying on NGINX for web services.

The implications for the financial services sector are substantial, as the hijacking of web traffic can lead to data breaches, loss of customer trust, and potential regulatory repercussions. Financial institutions must be vigilant in monitoring their NGINX configurations and implement robust security measures to mitigate the risk of such attacks.

Technical Details

- The campaign exploits the React2Shell vulnerability (CVE-2025-55182) to gain initial access via remote code execution.
- Attackers deploy a toolkit that includes scripts for injecting malicious configurations into NGINX.

- The malicious configurations are designed to redirect traffic from legitimate users to attacker-controlled servers.
- Key directives used in the malicious configurations include "proxy_pass", "rewrite", and "proxy_set_header".
- The toolkit operates in multiple stages, including orchestrating the attack and performing targeted injections.
- The final stage involves exfiltrating data about hijacked domains to the attacker's command and control server.
- The campaign utilizes obfuscated methods to evade detection, such as using Bash functions for data transfer.
- NGINX configuration files are modified to maintain persistence and redirect traffic without raising immediate alarms.

Recommendations

- Regularly audit and review NGINX configurations to identify unauthorized changes.
- Implement monitoring solutions to detect modifications to critical configuration files.
- Ensure that security patches for known vulnerabilities, such as React2Shell, are applied promptly.
- Utilize web application firewalls to filter and monitor incoming traffic for suspicious patterns.
- Train staff on security best practices related to web server management and incident response.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Active Web Traffic Hijacking Campaign Targets NGINX Installations

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
macOS Phishing Campaign Exploits AppleScript	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Darktrace security researchers have identified a phishing campaign targeting macOS users, utilizing AppleScript loaders and attempting to abuse the Transparency, Consent, and Control (TCC) privacy feature. The campaign employs social engineering tactics to manipulate user trust, enabling attackers to gain privileged access without exploiting system vulnerabilities.

This incident is significant because it highlights a shift towards social engineering over technical exploitation. The ability of malware to achieve persistence and access sensitive data through trusted applications poses a substantial risk to financial institutions, which must remain vigilant against such sophisticated phishing techniques.

Technical Details

- The infection chain begins with a phishing email prompting users to download an AppleScript file disguised as a Microsoft document.
- The AppleScript requires user interaction to execute, using social engineering to convince users to run the script.
- Once executed, the script sends system information to a remote server and retrieves additional malicious payloads.
- The malware establishes persistence using LaunchAgents and executes a modular Node[.]js loader to maintain long-term access.
- It attempts to manipulate the TCC database to gain unauthorized permissions for sensitive operations like screen recording and full disk access.
- The malware forges TCC authorizations for trusted binaries, allowing it to execute malicious actions without user consent.
- The campaign highlights a trend where attackers exploit user trust rather than system vulnerabilities to deliver malware.
- The malicious payloads are designed to steal user credentials and maintain communication with a command-and-control server.

Recommendations

- Implement user training programs to raise awareness about phishing tactics and the risks of executing unknown scripts.
- Regularly update macOS systems to ensure the latest security features and patches are applied.
- Utilize endpoint detection and response (EDR) solutions to monitor for suspicious script execution and unauthorized access attempts.
- Enforce strict permission controls and regularly audit application access to sensitive data.
- Deploy multi-factor authentication (MFA) to protect user accounts from credential theft.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – macOS Phishing Campaign Exploits AppleScript

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 Clickfix Variant 'CrashFix' Deploys Python Remote Access Trojan	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Microsoft Defender Experts have identified a new evolution in the ClickFix campaign, known as 'CrashFix', which deliberately crashes victims' browsers to lure them into executing malicious commands. This tactic combines user disruption with social engineering to enhance execution success while minimizing reliance on traditional exploit techniques. This new variant emerges as part of the multiple ClickFix campaigns observed since 2024, reflecting the continued evolution and refinement of this rapidly expanding social-engineering tactic.

This development is significant as it highlights the increasing sophistication of cyber threats. The use of social engineering alongside legitimate system utilities poses a serious risk, necessitating heightened awareness and behavior-based detection strategies to mitigate potential impacts on sensitive financial operations.

Technical Details

- The attack begins when victims search for ad blockers and encounter a malicious advertisement redirecting them to a harmful browser extension.
- The malicious extension impersonates a legitimate ad blocker "uBlock Origin Lite", creating a false sense of security for users.
- The payload employs a delayed execution technique, causing browser disruptions only after a period to obscure its origin.
- The attack utilizes the legitimate Windows utility finger[.]exe, which is renamed to ct[.]exe to evade detection.
- ct[.]exe connects to an attacker-controlled IP address to retrieve obfuscated PowerShell commands.
- The PowerShell script downloads additional payloads and checks for security tools to avoid detection.
- The core malicious functionality includes a Remote Access Trojan (RAT) that communicates with the command-and-control server via periodic beacons.
- The RAT establishes persistence by creating a Run registry entry, ensuring execution at user login.
- The attacker bundles a complete Python environment to facilitate reliable execution across compromised systems.
- The campaign demonstrates a selective deployment of payloads based on the target's environment, particularly for domain-joined systems.

Recommendations

- Enable cloud-delivered protection in antivirus products to guard against evolving threats.
- Implement endpoint detection and response (EDR) in block mode to remediate detected malicious artifacts.

- Apply network egress filtering to restrict unnecessary outbound access and limit misuse of system utilities.
- Encourage the use of browsers with SmartScreen to block malicious websites and phishing attempts.
- Enforce multi-factor authentication (MFA) across all accounts and devices to enhance security.

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
Critical Remote Command Execution Vulnerability in n8n Workflow Automation Platform	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

A critical security vulnerability has been identified in the n8n workflow automation platform, tracked as CVE-2026-25049. This flaw allows an authenticated user with workflow creation or modification privileges to execute arbitrary system commands on the underlying server, potentially exposing the system to unauthorized access. The vulnerability is a bypass of previous protections and, when combined with n8n's public webhook feature, can enable remote code execution by unauthenticated external users.

This vulnerability may be a concern for parts of the financial services sector, given the potential for unauthorized access and manipulation of sensitive workflows. Financial institutions utilizing n8n for automation must prioritize immediate upgrades to secure their systems, as the exploitation of this vulnerability could result in significant operational disruptions and data breaches.

Technical Details

- CVE ID: CVE-2026-25049, with a CVSS score of 9.4 indicating critical severity.
- The flaw allows authenticated users to execute arbitrary commands on the server through crafted expressions in workflows.
- This vulnerability bypasses protections from a previous critical issue, CVE-2025-68613.
- Attackers can exploit the vulnerability by leveraging n8n's public webhook feature to expose malicious workflows.
- Affected versions include n8n versions prior to 1.123.17 and 2.5.2.

Recommendations

- Upgrade n8n immediately to one of the fixed versions or the latest version to mitigate risks.
- Restrict workflow creation and editing to fully trusted users only to limit exposure.
- Disable or tightly control public webhooks to prevent unauthorized access.

- Deploy n8n in a hardened environment by running with minimal OS privileges and applying strict network segmentation.
- Monitor for unexpected workflow changes, suspicious webhook activity, and abnormal system commands or processes.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High Severity SQL Injection Vulnerability in ManageEngine ADSelfService Plus	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

ManageEngine ADSelfService Plus has been found to contain a high-severity SQL injection vulnerability, tracked as CVE-2026-1367. This vulnerability can be exploited by authenticated technicians through the Reports module, allowing for the execution of arbitrary SQL commands. Such exploitation could lead to unauthorized modifications of databases and compromise sensitive identity-related data.

This vulnerability may raise concerns in parts of the financial services sector, given the potential exposure of sensitive customer information and the risk of data compromise. Organizations using ManageEngine ADSelfService Plus are urged to take immediate action to mitigate the risks associated with this vulnerability to protect their data integrity and customer trust.

Technical Details

- CVE ID: CVE-2026-1367 indicates a high-severity SQL injection vulnerability in ManageEngine ADSelfService Plus.
- The vulnerability allows authenticated technicians to exploit the Reports module through improperly sanitized custom input.
- Successful exploitation could enable the execution of arbitrary SQL commands against the database.
- This could result in unauthorized modifications to the database and compromise sensitive identity-related data.
- Affected versions include ManageEngine ADSelfService Plus builds 6522 and earlier.

Recommendations

- Upgrade to ManageEngine ADSelfService Plus Build 6523 immediately 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
Google Chrome Vulnerabilities Enabling Remote Code Execution	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Google has released a security update for the Chrome browser addressing multiple high-severity vulnerabilities, including a heap buffer overflow and a type confusion vulnerability. These vulnerabilities could allow attackers to execute arbitrary code or crash the browser through malicious web content.

Successful exploitation may pose risks to some users in the financial services sector, potentially enabling system compromise and unauthorized access to sensitive information. Financial institutions should prioritize updating their browsers to mitigate these risks.

Technical Details

- CVE-2026-1861 is a high-severity heap buffer overflow in libvpx, allowing memory corruption via specially crafted media content.
- CVE-2026-1862 is a high-severity type confusion vulnerability in the V8 JavaScript engine, potentially enabling arbitrary code execution in the browser context.
- Exploitation of these vulnerabilities could lead to remote code execution, crashing the browser, or system compromise.
- Attackers may exploit these vulnerabilities through malicious web content, increasing the need for vigilance in browsing practices.
- The vulnerabilities affect multiple platforms, including Windows, Mac, Linux, and Android versions of Chrome.

Recommendations

- Update Google Chrome to the latest version immediately to mitigate vulnerabilities.

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	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Cisco has released security updates to address several vulnerabilities affecting its TelePresence and RoomOS Software, Cisco Meeting Management, and other products. These vulnerabilities, which include

Denial of Service (DoS), Arbitrary File Upload, and Cross-Site Scripting (XSS), could allow attackers to disrupt services, upload malicious files, or execute client-side attacks.

The implications for financial services may be notable, as these vulnerabilities could lead to service disruptions and unauthorized access to sensitive data. Financial institutions utilizing these Cisco products must prioritize applying the recommended security updates to mitigate potential risks.

Technical Details

- Cisco TelePresence Collaboration Endpoint Software and RoomOS has a DoS vulnerability (CVE-2026-20119) that could render devices unresponsive, requiring manual restarts.
- Cisco Meeting Management contains an arbitrary file upload vulnerability (CVE-2026-20098) that could allow authenticated attackers to upload malicious files, risking remote code execution.
- The Cisco Secure Web Appliance has a medium severity vulnerability (CVE-2026-20056) that allows crafted archive files to bypass real-time malware scanning, increasing malware infection risks.
- Cisco Prime Infrastructure is affected by a stored XSS vulnerability (CVE-2026-20111), enabling authenticated attackers to inject malicious scripts that execute in users' browsers.
- An open redirect vulnerability (CVE-2026-20123) exists in Cisco EPNM and Cisco Prime Infrastructure, allowing unauthenticated attackers to redirect users to malicious web pages.

Recommendations

- Apply the security updates provided by Cisco to mitigate the identified vulnerabilities.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Vulnerabilities Discovered in Django Framework	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

The Django Security Team has released urgent security updates addressing six vulnerabilities that impact supported versions of the Django framework. These vulnerabilities include three high-severity SQL injection flaws, two denial-of-service vulnerabilities, and one username enumeration weakness, which could potentially affect applications within the financial services sector that rely on Django for web development.

This may raise concerns for financial institutions, as it could allow unauthorized access to sensitive data, disrupt services, and enable misuse of user accounts. Timely patching is essential to mitigate these risks and ensure the integrity and availability of financial services applications.

Technical Details

- CVE-2026-1207: High-severity SQL injection vulnerability via Raster Lookups on PostGIS untrusted band index input, allowing arbitrary SQL execution.

- CVE-2026-1287: High-severity SQL injection in Column Aliases through Control Characters FilteredRelation, enabling crafted column aliases to execute SQL injection.
- CVE-2026-1312: High-severity SQL injection via QuerySet[.]order_by() with FilteredRelation, where column aliases containing periods can be exploited.
- CVE-2025-14550: Moderate denial-of-service vulnerability via repeated headers in ASGI, leading to service degradation or outages.
- CVE-2026-1285: Moderate denial-of-service vulnerability in HTML Truncator, where unmatched HTML end tags cause quadratic parsing time.
- CVE-2025-13473: Low-severity username enumeration vulnerability via mod_wsgi, allowing remote attackers to enumerate valid usernames through timing attacks.
- The vulnerabilities affect applications built on the Django framework.

Recommendations

- Upgrade Django immediately to one of the fixed versions provided by the Django Security Team.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
CrossCurve Bridge Hacked, Resulting in $3 Million Loss	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

CrossCurve, a cross-chain liquidity protocol, has reported a significant security breach involving the exploitation of a vulnerability in its smart contract. Attackers successfully bypassed gateway verification, leading to unauthorized access and a drastic reduction of the pool's balance from $3 million to nearly zero. The developers have advised users to refrain from interacting with the platform during the investigation.

This incident underscores the vulnerabilities present in decentralized finance (DeFi) protocols, particularly those utilizing smart contracts. As financial services increasingly integrate blockchain technology, the implications of such breaches can be profound, affecting user trust and financial stability within the sector.

Technical Details

- Hackers exploited a vulnerability in the ReceiverAxelar smart contract(a custom smart contract developed by the CrossCurve team), allowing them to bypass gateway verification.
- The attackers used spoofed cross-chain messages to invoke the expressExecute function.
- This exploitation enabled unauthorized unlocking of tokens in the PortalV2 contract.
- The balance of the CrossCurve pool dropped from $3 million to nearly zero following the breach.
- CrossCurve employs a Consensus Bridge mechanism that relies on independent protocols for transaction verification.

- The incident raises concerns about the security of cross-chain protocols and their susceptibility to simultaneous attacks.

Recommendations

- Organizations that develop, deploy, or rely on smart contracts should conduct thorough audits to identify and remediate vulnerabilities.
- Educate users on the risks associated with interacting with decentralized protocols, especially during known incidents.
- Collaborate with security experts to enhance the security posture of blockchain-based services.

Reference to the Source

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Cloud File-Sharing Abuse in a Coordinated Phishing Campaign Delivering Remcos RAT Targeting the UAE

Tactic	Technique
Initial Access	Phishing (T1566)
Resource Development	Compromise Infrastructure (T1584)
Execution	Command and Scripting Interpreter (T1059)
Execution	User Execution (T1204)
Persistence	Scheduled Task/Job (T1053)
Defense Evasion	Obfuscated Files or Information (T1027)
Defense Evasion	Process Injection (T1055)
Defense Evasion	Masquerading (T1036)
Defense Evasion	Deobfuscate/Decode Files or Information (T1140)
Discovery	System Information Discovery (T1082)
Discovery	Browser Information Discovery (T1217)
Command & Control	Application Layer Protocol (T1071)
Command & Control	Ingress Tool Transfer (T1105)
Command & Control	Non-Standard Port (T1571)
Collection	Input Capture (T1056)
Collection	Screen Capture (T1113)
Collection	Archive Collected Data (T1074)
Credential Access	Credentials from Password Stores (T1555)
Exfiltration	Exfiltration Over C2 Channel (T1041)

APT28 Campaign Operation Neusploit Exploits CVE-2026-21509

Tactic	Technique
Initial Access	T1566.001 - Phishing: Spear phishing Attachment
Execution	T1203 - Exploitation for Client Execution
Execution	T1106 - Native API
Execution	T1053.005 - Scheduled Task/Job: Scheduled Task
Execution	T1204.002 - User Execution: Malicious File
Persistence	T1546.015 - Event Triggered Execution: Component Object Model Hijacking
Persistence	T1137.002 - Office Application Startup: Add-ins
Defense Evasion	T1140 - Deobfuscate/Decode Files or Information
Defense Evasion	T1480.001 - Execution Guardrails: Mutual Exclusion
Defense Evasion	T1027.007 - Obfuscated Files or Information: Dynamic API Resolution
Defense Evasion	T1027.003 - Obfuscated Files or Information: Steganography
Defense Evasion	T1497.003 - Virtualization/Sandbox Evasion: Time Based Checks
Collection	T1114 - Email Collection
Command and Control	T1071.001 - Application Layer Protocol: Web Protocols
Command and Control	T1102.002 - Web Service: Bidirectional Communication

Rublevka Team Engages in Large-Scale Cryptocurrency Theft Using Sophisticated Drainer Operations

Tactic	Technique
Initial Access	T1566 - Phishing
Defense Evasion	T1027 - Obfuscated Files or Information
Command and Control	T1071.001 - Application Layer Protocol, Web Protocols
Command and Control	T1568.002 - Dynamic Resolution, Domain Generation Algorithms
Command and Control	T1665 - Hide Infrastructure
Impact	T1657 - Financial Theft

Active Web Traffic Hijacking Campaign Targets NGINX Installations

Tactic	Technique
Initial Access	T1190 - Exploit Public-Facing Application
Execution	T1059.004 - Command and Scripting Interpreter: Unix Shell
Persistence	T1505.004 - Server Software Component: IIS Components (Nginx equiv.)
Defense evasion	T1027 - Obfuscated Files or Information
Discovery	T1083 - File and Directory Discovery
Discovery	T1082 - System Information Discovery
Collection	T1557 - Adversary-in-the-Middle (AiTM)
Exfiltration	T1041 - Exfiltration Over C2 Channel

macOS Phishing Campaign Exploits AppleScript

Tactic	Technique
Execution	T1059.002 - Command and Scripting Interpreter: AppleScript
Execution	T1059.004 - Command and Scripting Interpreter: Unix Shell
Execution	T1059.007 - Command and Scripting Interpreter: JavaScript
Defense Evasion / Privilege Escalation	T1222.002 - File and Directory Permissions Modification
Defense Evasion	T1036.005 - Masquerading: Match Legitimate Name or Location
Defense Evasion	T1140 - Deobfuscate/Decode Files or Information
Persistence / Privilege Escalation	T1547.001 - Boot or Logon AutoStart Execution: Launch Agent
Defense Evasion / Privilege Escalation	T1553.006 - Subvert Trust Controls: Code Signing Policy Modification
Discovery	T1082 - System Information Discovery
Discovery	T1057 - Process Discovery
Command and Control	T1105 - Ingress Tool Transfer
Initial Access	T1566 - Phishing

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
.tar archive	Compressed package used to deliver multiple JavaScript droppers for redundancy
/open-url endpoint	API path abused to trigger remote OS command execution on Metro servers
Access controls (development servers)	Limiting who can reach dev servers to reduce exposure
Advanced endpoint protection	Defensive tooling recommended to catch PowerShell-based attacks
Affiliates / Commission rates	Program details that incentivize broader participation in scams
AppleScript loader (macOS)	Initial script delivered via phishing that sends system info and pulls more payloads
APT28 (threat actor)	Actor behind Operation Neusploit using crafted Microsoft RTF files to deploy backdoors and steal emails
Arbitrary file upload	Flaw allowing authenticated attackers to upload malicious files
Arbitrary SQL commands	Ability to modify databases and compromise identity-related data
Arbitrary system command execution	Outcome where attackers can run any command on the underlying server
ASGI repeated headers	Issue that can lead to denial of service in Django

Automated infrastructure	Actor tooling for landing page creation, campaign tracking, and defenses
Backend server (attacker-controlled)	Destination to which hijacked traffic is redirected
Baota (management panel)	Management panel cited as a target alongside NGINX in the hijacking campaign
Base64-encoded payload	Encoding style used so scripts can be decoded and executed after delivery
Bash functions (obfuscated transfer)	Stealthy method used for data transfer and evasion
Bitget (impersonation)	Legitimate crypto service the actor mimics
Blocklist for C2 IP addresses	Recommendation to block known attacker command-and-control servers
Brand impersonation	Phishing messages posing as known companies to increase victim trust
Build 6523 (upgrade)	Version referenced as the fix for the vulnerability
Bundled Python environment	Packaging a full Python setup to ensure the payload runs reliably
Chrysalis (backdoor)	Custom backdoor delivered via the Notepad++ update compromise to maintain covert access
Cisco EPNM	Product referenced as affected by an open redirect vulnerability
Cisco Meeting Management	Product with an arbitrary file upload vulnerability that could allow malicious files to run
Cisco Prime Infrastructure	Product impacted by stored XSS and open redirect vulnerabilities
Cisco Secure Web Appliance	Product where crafted archives can bypass real-time malware scanning
Cisco TelePresence Collaboration Endpoint Software	Product with a DoS vulnerability that can render devices unresponsive
ClickFix / CrashFix (campaign)	Technique that deliberately crashes browsers to coerce users into executing attacker commands
Cloud-based file-sharing abuse	Use of a legitimate cloud service to host or deliver malware and bypass filters
Cloud-delivered protection	Antivirus capability recommended to react to emerging threats quickly
cmd.exe	Windows command interpreter used to launch the PowerShell loader
Cobalt Strike	Commodity tool observed alongside the custom backdoor during the Notepad++ compromise
colorcpl.exe (EDR cue)	Legitimate Windows binary whose unusual child-process behaviour should trigger alerts
Column Aliases with FilteredRelation	Mechanism enabling SQL injection in the cited CVE
COM object hijacking	Persistence method abused by PixyNetLoader
Command and Control (C2) communications	Attacker infrastructure used to manage compromised systems; several entries advise blocking C2 IPs
Command-and-control server (macOS campaign)	Remote server used to receive data and send additional payloads
Connect wallet authorization	Prompt that, when approved, enables the fraudulent transfer of funds
Consensus Bridge	Mechanism relying on independent protocols for transaction verification in CrossCurve
CPX-TIC	CPX Threat Intelligence Center
Crasher mode	Drainer behaviour used to manipulate interactions and obscure theft
Credential harvesting	Theft of usernames and passwords enabled by the malware
Cross-chain liquidity protocol	Service model used by CrossCurve for moving assets across chains
CrossCurve	Cross-chain liquidity protocol that suffered a breach reducing the pool balance from about $3M to nearly zero
Cross-Site Scripting (XSS)	Client-side script injection noted in Cisco advisories
CSC	UAE Cyber Security Council
ct.exe (renamed utility)	Renamed finger exe used to fetch obfuscated PowerShell commands
CVE-2025-11953	Vulnerability in the Metro Development Server enabling unauthenticated remote command execution

CVE-2025-13473 (mod_wsgi username enumeration)	Low-severity ability to enumerate valid usernames via timing
CVE-2025-14550 (ASGI repeated headers)	Moderate DoS via repeated headers causing degradation or outages
CVE-2025-68613 (prior issue)	Earlier critical n8n issue whose protections were bypassed by the new flaw
CVE-2026-1207 (PostGIS Raster Lookups)	High-severity SQL injection via untrusted band index input
CVE-2026-1285 (HTML Truncator)	Moderate DoS due to quadratic parsing time with unmatched end tags
CVE-2026-1287 (Column Aliases / FilteredRelation)	High-severity SQL injection through crafted column aliases
CVE-2026-1312 (QuerySet.order_by with FilteredRelation)	High-severity SQL injection via column aliases containing periods
CVE-2026-1367	SQL injection in the Reports module allowing authenticated technicians to run arbitrary SQL
CVE-2026-21509	Critical vulnerability exploited via Microsoft RTF files in Operation Neusploit
CVE-2026-25049	Critical n8n vulnerability; a bypass of protections from CVE-2025-68613 and can enable remote code execution via public webhooks
Darktrace	Team reporting the macOS AppleScript phishing campaign
Data exfiltration	Unauthorized removal of data noted as a risk in multiple campaigns
Datadog Security Research	Team identifying the active NGINX web-traffic hijacking campaign
DDoS protection (malicious infrastructure)	Feature mentioned as part of the actor's tooling to protect their sites
Decentralized Finance (DeFi)	Sector context for the CrossCurve incident and broader smart-contract risk
Delayed execution (crash tactic)	Waiting before causing browser disruption to obscure the source
Denial of Service (DoS)	Condition where services become unavailable; cited in Cisco and Django items
Django framework	Web framework with multiple fixes for SQL injection, DoS, and username enumeration
Django Security Team	Team releasing urgent security updates for supported Django versions
DLL sideloading	Technique abusing how Windows loads DLLs so malicious code runs alongside legitimate executables
Domain rotation	Regular switching of domains to avoid takedowns and detection
Domain-joined systems	Enterprise devices where payload deployment may vary based on environment checks
EDR in block mode	Setting where EDR can automatically stop and remediate detected malicious activity
Email filtering (business-themed lures)	Strengthening filters to flag external emails that mix business themes with external hosting links
Email stealer (Outlook)	Functionality to extract emails from Outlook
Encrypted payloads	Payloads that are decrypted and executed on the victim system
Encrypted shellcode	Obfuscated machine code decrypted at runtime as part of the attack chain
Endpoint Detection and Response (EDR)	Endpoint security tooling referenced for detecting and blocking suspicious activities
Exfiltration of hijacked domain data	Sending details about compromised sites to attacker C2
expressExecute function	Smart-contract function invoked to unlock tokens
FileCloudTrial subdomain	Specific cloud subdomain abused to host or deliver payloads in the UAE campaign
finger.exe	Legitimate Windows utility used in the attack chain
Gateway verification (bypass)	Check that was bypassed to gain unauthorized access in the breach
Google Chrome	Browser receiving security updates for multiple high-severity issues
Hardcoded 1-byte XOR key	Simple decryption method referenced in MiniDoor
Hardened deployment	Running n8n with minimal OS privileges and strict segmentation

Heap buffer overflow (libvpx)	Memory corruption issue tracked as CVE-2026-1861
Honeypot mode	Drainer behaviour used to manipulate interactions and obscure theft
HTML Truncator unmatched end tags	Condition causing excessive parsing time and service impact
Impersonation of “uBlock Origin Lite”	Fake extension name used to appear trustworthy
Indicators of Compromise (IOCs)	Concrete artifacts (e.g., file paths, hashes, patterns) used for threat hunting and detection
Insikt Group	Team identifying the “Rublevka Team” cryptocurrency theft operation
JavaScript dropper	Obfuscated script (with junk-code padding) that initiates the infection chain and persistence
Junk-code padding (obfuscation)	Extra meaningless code added to scripts to evade detection
LaunchAgents	macOS mechanism used to achieve persistence and start at login
libvpx	Media library referenced in the Chrome vulnerability
Living-off-the-Land techniques	Abusing legitimate Windows processes to evade behavioural monitoring
Localized lures (social engineering)	Tailored bait content used to increase success rates
LolzTeam (forum)	Online forum where the actor operates and recruits affiliates
Malicious advertisement (search result)	Ad that redirects users looking for ad blockers to a harmful extension
Malicious macros (Outlook)	Macro-based mechanism used to run attacker code automatically in Outlook
Malicious update manifests	Tampered update instructions used to push attacker payloads instead of legitimate updates
Malicious web content	Content that could trigger code execution or crashes in vulnerable browsers
ManageEngine ADSelfService Plus	Identity-related product affected by a high-severity SQL injection
Metasploit	Commodity tool observed alongside the custom backdoor during the Notepad++ compromise
Microsoft Defender exclusions	Paths added by the payload, so defenses skip scanning
Microsoft Defender Experts	Team identifying the ClickFix “CrashFix” evolution
Microsoft RTF files	Document files used to initiate exploitation in this campaign
MiniDoor (dropper)	Lightweight DLL that targets Microsoft Outlook to steal emails
Minimal OS privileges	Limiting operating system rights to reduce impact if compromised
mod_wsgi username enumeration	Technique allowing attackers to infer valid usernames
Monitor workflow changes / webhooks	Watching for unexpected changes and suspicious webhook activity
Monitoring configuration changes	Recommended practice to catch unauthorized edits to NGINX files
Multi-Factor Authentication (MFA)	An added login step recommended across multiple entries to reduce unauthorized access
Multi-stage loader chain	Stepwise execution process used to load malware components while evading detection
Mutex	Execution object created by malware during operation
n8n (workflow automation platform)	Platform affected by a critical flaw that lets privileged users run system commands
Network egress filtering	Restricting outbound connections so malware cannot freely reach attacker servers
Network segmentation	Separating systems to limit lateral movement and blast radius
NGINX configuration injection	Scripts inject malicious directives into NGINX to redirect traffic and persist
Node.js loader (modular)	Component executed after initial access to maintain long-term control
Notepad++ update service / infrastructure	The update distribution path for Notepad++ that was compromised to redirect update traffic to attacker payloads
Obfuscated PowerShell	Script used to download payloads and check for security tools
Open redirect	Flaw allowing redirection to attacker-controlled pages

Operation Neusploit	APT28 campaign exploiting CVE-2026-21509 and dropping MiniDoor and PixyNetLoader
Operational disruption	Business impact emphasized for several items (e.g., traffic hijacking, phishing, browser crashes)
Permission controls (macOS)	Enforcement and audits recommended for access to sensitive data and features
Persistence in NGINX conf files	Modifications that keep malicious redirects in place without obvious alarms
Phantom (impersonation)	Legitimate crypto service the actor mimics
PixyNetLoader (dropper)	More complex loader using checks and COM object hijacking for persistence
PortalV2 contract	Contract where tokens were unlocked after the bypass
Ports 9551 and 9558	Outbound ports recommended for blocking in response to the Remcos campaign
POST request	HTTP method used to interact with the vulnerable endpoint in this exploitation
PostGIS untrusted band index input	Vector allowing arbitrary SQL execution in the cited CVE
PowerShell-based loader	Multi-stage script executed via cmd.exe to establish access and evade defenses
Process execution chains	Sequences of processes whose behaviour reveals potentially malicious activity
Promotions / Airdrops (lures)	Offers used to entice victims to malicious pages
proxy_pass directive	NGINX directive abused to forward requests to attacker-controlled backends
proxy_set_header directive	NGINX directive abused to manipulate headers in redirected traffic
Public webhook (n8n)	Feature which, if exposed, can allow unauthenticated external triggering of malicious workflows
QuerySet.order_by() with FilteredRelation	Code path referenced as vulnerable to SQL injection
Randomized filenames	A tactic used to evade signature-based detection
RAT with periodic beacons	Malware component that regularly checks in with its controller
Raw TCP connection	Direct network connection established to an attacker-controlled host
React Native Metro Development Server	Development server targeted to run OS commands without authentication via a specific endpoint
React2Shell (CVE-2025-55182)	Exploit path used to gain initial access before modifying NGINX configurations
Real-time malware scanning bypass	Issue where crafted archives evade scanning in Cisco Secure Web Appliance
Registry modifications	Changes enabling malicious macros to load and to maintain persistence
Remcos RAT (Remote Access Trojan)	Final payload granting remote access, keystroke logging, and credential harvesting
Reports module (ManageEngine)	Component through which improperly sanitized input can be abused
rewrite directive	NGINX directive abused to change request paths for hijacking
RoomOS	Cisco product referenced with the TelePresence DoS issue
RPC APIs	Interfaces the group exploits as part of scaling drainer operations
Rublevka Team (threat actor)	Group conducting large-scale wallet-draining operations using spoofed pages and social engineering
Run registry entry	Windows registry location used to start the malware at user login
Scheduled task (persistence)	Repeated system job created by malware to survive reboots and maintain access
Security assessments (dev environments)	Regular reviews of development environments to identify weaknesses
Security tool checks	Technique to avoid running when defenses are detected
Service/registry persistence artifacts	System changes attackers use to survive reboots and maintain presence
Shared hosting server (compromise)	The server hosting the Notepad++ update service was compromised, enabling interception and redirection
Smart contract (CrossCurve)	Code with a flaw that allowed attackers to bypass gateway verification

SmartScreen	Browser protection recommended to block malicious websites and phishing attempts
SOL assets	Digital assets specifically referenced as being exfiltrated by the drainer
Spoofed cross-chain messages	Fake messages used to invoke privileged functions on the contract
Spoofed landing pages	Fake sites that mimic legitimate crypto services to build trust
Supply-chain attack	Abusing a trusted software update path (e.g., Notepad++ updates) to deliver malicious payloads to selected victims
TCC (Transparency, Consent, and Control)	macOS privacy feature the campaign attempts to manipulate to gain privileged access
Telegram channel	Communication venue associated with reporting and organizing wallet drains
Threat hunting	Proactive searches across endpoints and network telemetry to find signs of the listed campaigns
Trusted binaries (forged authorizations)	Abuse where malware makes macOS treat actions as approved by trusted apps
Type confusion (V8)	JavaScript engine issue tracked as CVE-2026-1862 that can enable code execution
V8 JavaScript engine	Engine affected by the type confusion vulnerability
VulnCheck	Team that observed active exploitation of CVE-2025-11953 against the Metro server
Wallet drainer (JavaScript drainer)	Code on spoofed pages that tricks users into authorizing fraudulent wallet transactions
Web application firewall	Control recommended to filter and monitor web traffic for suspicious patterns
Web traffic hijacking (NGINX)	Attackers alter NGINX configurations to silently redirect user traffic to attacker servers
WinGup certificate/signature verification	Update verification control recommended to prevent unauthorized Notepad++ updates
Workflow creation/modification privileges	n8n access level that enables exploitation of the vulnerability
Zscaler ThreatLabz	Team attributing Operation Neusploit to APT28