TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	9/4/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

WEEKLY SUMMARY REPORT – 9 April 2026

8	6	1	0
Campaigns	**Vulnerability**	**Cyber Breach**	**Threat Actors**
Threat Campaigns of Potential Relevance to Finance Sector	Actively Exploited & Critical Vulnerabilities	Major Compromises and Breaches	Threat actor activities in the Middle East impacting Finance Sector

Summary

This week's cybersecurity newsletter highlights a convergence of destructive attacks, stealthy intrusion techniques, high-impact breaches, and actively exploited vulnerabilities affecting browsers, endpoint management platforms, enterprise infrastructure, cloud services, and web applications. Key developments include large-scale data-destructive wiper malware, a USD *"285 million"* breach of a decentralized trading platform, covert cookie-controlled PHP web shell activity on Linux servers, and multiple critical vulnerabilities with confirmed exploitation in widely deployed technologies. For organizations in the financial sector, these issues may impact operational resilience, digital asset exposure, endpoint security, and cloud-hosted services. Stakeholders should focus on timely patching, better visibility across managed services and web platforms, stronger access controls, and solid governance, while ensuring preparedness for both destructive attacks and financially motivated intrusions that exploit trust, identity, and configuration weaknesses.

ADGM THREAT INTELLIGENCE SUMMARY

Name	Threat Severity Rating	TLP	Attribution	Originating Source
UAT-10608 Automated Credential Harvesting Campaign Exploiting Web Applications	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an automated credential harvesting campaign carried out by a threat cluster tracked as UAT-10608, targeting publicly exposed web applications. The campaign is targeting Next.js applications vulnerable to React2Shell (CVE-2025-55182). This activity leverages the vulnerability to gain unauthenticated remote code execution, followed by the deployment of an automated framework designed to collect credentials and sensitive configuration data at scale.

This campaign may impact organizations in the financial sector that operate internet-facing web applications, as harvested credentials could affect access to cloud services, application backends, and third-party platforms. Organizations in financial services should be aware of the potential exposure created by vulnerable application deployments and the downstream risks associated with compromised secrets.

Technical Details

- The campaign begins with large-scale automated scanning to identify publicly reachable web applications that expose vulnerable server-side components.
- When a vulnerable application is found, attackers send a specially crafted web request that triggers remote code execution without requiring authentication.
- Successful exploitation provides direct access to the server-side application runtime, allowing malicious scripts to execute immediately.
- A multi-phase automated harvesting script is deployed to systematically collect sensitive data from the compromised environment.
- The script gathers environment variables and application secrets that may include API keys, authentication tokens, and configuration values.
- It also extracts SSH keys and shell command history, which can reveal additional credentials or enable further access.
- Cloud environment metadata services are queried to obtain temporary or persistent credentials associated with the affected workload.
- Containerized environments are inspected to collect information about running services, images, and runtime configurations.
- Harvested data is segmented and transmitted to external infrastructure controlled by the threat actor over standard web protocols.
- Stolen information is aggregated into a centralized web-based interface that allows operators to review and manage compromised hosts at scale.

Recommendations

- Review and remediate internet-facing web applications for vulnerable configurations referenced in the campaign.
- Rotate credentials, tokens, and secrets accessible to affected applications, particularly those tied to cloud and third-party services.
- Restrict access to environment variables and metadata services to only what is operationally required by applications.
- Monitor server-side application behavior for unexpected script execution and abnormal outbound network activity.
- Strengthen logging and detection around automated scanning attempts and unusual web request patterns targeting application endpoints.

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
Password Spray Campaign Targeting Cloud Environments in the Middle East	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a password-spraying campaign targeting Microsoft 365 environments, with a primary focus on the Middle East. The activity consists of repeated authentication attempts against cloud tenants using common passwords, executed in multiple coordinated waves, and routed through anonymization infrastructure to evade detection.

This campaign may impact organizations in the financial sector that rely on cloud identity platforms, as weak or reused credentials could affect access to email, documents, and administrative cloud resources. Organizations in the financial sector should be aware of this activity, particularly where cloud authentication controls and password hygiene are insufficiently enforced.

Technical Details

- The activity was observed as a series of distinct attack waves conducted over multiple dates, indicating a planned and coordinated operation.
- Attackers targeted cloud identity services by attempting common or weak passwords across many user accounts rather than focusing on a single account.
- This password-spraying approach reduces lockouts and helps blend malicious attempts into background authentication traffic.
- Login attempts were distributed across multiple source IP addresses, making detection based on static indicators more difficult.

- Traffic was routed through anonymization infrastructure to frequently change source locations and avoid simple blocking.
- The campaign primarily focused on cloud tenants located in the Middle East.
- Once valid credentials are identified, attackers can access cloud-hosted services without deploying malware or exploiting software vulnerabilities.
- Targeting patterns suggest a broad and automated effort rather than victim-specific reconnaissance.
- The overall operation reflects an identity-focused access strategy centered on exploiting weak authentication controls.

Recommendations

- Enforce strong password policies across all cloud user accounts, including restrictions on commonly used passwords.
- Implement and require multi-factor authentication for cloud access, particularly for privileged and externally accessible accounts.
- Monitor cloud authentication logs for patterns consistent with password spraying, such as low-and-slow login failures across many users.
- Apply conditional access controls to limit sign-ins based on geography or risk signals where appropriate.
- Regularly review and audit cloud tenant security posture to identify and remediate authentication weaknesses.

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
Wiper Malware Campaign Targeting Multiple Sectors	HIGH	CLEAR	Campaign	CSC

Executive Summary

It has been observed that an active and ongoing wiper malware campaign has re-emerged, targeting organizations across multiple sectors in the region. The malware is designed to irreversibly delete data, disable systems, and destroy files and backups to prevent recovery, leading to significant operational disruption. Attackers likely gain initial access via phishing, stolen credentials, or unpatched vulnerabilities, and then move laterally using remote admin tools, SMB shares, and elevated domain privileges.

This campaign may impact organizations in the financial sector due to its destructive nature and ability to propagate across networks using compromised access. Organizations in the financial sector should be aware that wiper malware incidents can affect core systems, disrupt critical operations, and significantly hinder recovery efforts.

Technical Details

- The campaign involves wiper malware whose primary function is permanent data destruction rather than financial extortion. The malware deletes files, corrupts system components, and intentionally renders systems inoperable.
- Affected environments have experienced system crashes and instances where machines fail to boot after execution. In several cases, both operational data and backups were deleted, limiting recovery options.
- The malware has been observed spreading beyond the initially compromised system in some incidents. This includes network-wide propagation using available credentials and shared resources.
- Initial access is believed to occur through phishing emails containing malicious attachments or links.
- Stolen or compromised credentials, including VPN access, are used to gain entry into internal networks.
- Unpatched vulnerabilities are also leveraged to expand access and move deeper into environments.
- Once malware is inside the network, lateral movement occurs through remote administration tools. Shared network resources such as SMB shares and domain privileges are abused to spread the malware.
- Administrative credentials are commonly used to accelerate propagation and execute destructive actions. This enables simultaneous impact across multiple systems.
- Suspicious command-line and PowerShell activity has been associated with the destructive phase of the attack. These actions precede large-scale file deletion and system destabilization.

Recommendations

- Enforce multi-factor authentication on all remote access and review the use of privileged accounts.
- Apply critical security patches promptly and restrict exposure of internet-facing systems.
- Segment networks to limit lateral movement and isolate critical systems from general user access.
- Maintain offline, immutable backups and regularly test restoration procedures.
- Increase endpoint and network monitoring to detect suspicious administrative and scripting activity.

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
North Korea-Nexus Backdoor Embedded in Axios NPM Package Supply Chain Attack	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a supply chain attack in which a threat actor compromised the Axios NPM package to distribute malicious code to downstream users. The attacker gained access to a legitimate maintainer account and released unauthorized package versions that introduced a hidden dependency designed to deploy a cross-platform backdoor during installation.

This activity may impact organizations in the financial sector that rely on open-source components within development pipelines or cloud-hosted applications. Organizations in the financial sector should be aware that compromised development or build environments could affect application integrity, cloud credentials, and sensitive operational workflows.

Technical Details

- The attack targeted the official Axios NPM package by compromising a trusted maintainer account used to publish new releases.
- Two unauthorized package versions were published to the NPM registry within a short time window before being removed.
- The malicious releases introduced a new dependency that was not required for Axios functionality and contained hidden malicious logic.
- During installation, the dependency executed an automatic post-install script without user interaction.
- The script acted as an obfuscated dropper that checked the operating system before delivering a platform-specific payload.
- Separate payloads were delivered for Windows, macOS, and Linux systems, enabling remote access to compromised hosts.
- The backdoor allowed attackers to execute commands, collect system information, and interact remotely with affected environments.
- After execution, the malware attempted to remove installation artifacts to reduce visibility and hinder forensic analysis.
- The attack leveraged trusted software distribution channels, allowing malicious code to spread through legitimate update mechanisms.
- Attribution analysis linked the tooling and infrastructure used in this campaign to a North Korea-nexus threat actor.

Recommendations

- Audit development, build, and production environments to identify affected package versions referenced in the campaign.
- Rebuild systems from trusted sources if compromised packages were installed during the exposure period.
- Rotate credentials, tokens, and secrets accessible to affected environments, including cloud and CI/CD credentials.
- Restrict automatic dependency updates and require integrity verification for third-party packages.
- Enhance monitoring around supply chain activity, including unexpected dependency changes or post-install behaviors.

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
EvilTokens Device Code Phishing Service Automates Token Theft and BEC	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a phishing-as-a-service platform known as EvilTokens, a Microsoft device code phishing kit that supports BEC attacks by enabling account takeover, email collection, reconnaissance, a built-in webmail interface, and automated workflows. The service automates the creation of phishing pages and backend infrastructure to trick users into completing legitimate authentication steps, resulting in direct token theft without password capture.

This campaign may impact organizations in the financial sector that rely heavily on cloud identity platforms, as stolen access tokens could affect email access and downstream business workflows. Organizations in the financial sector should be aware of the risk posed by token-based attacks that bypass traditional credential protections and enable follow-on business email compromise activity.

Technical Details

- The EvilTokens service abuses device code authentication flows, which are designed to allow sign-in without entering credentials on the device initiating the request.
- Victims are redirected to a phishing page that instructs them to legitimately authenticate using a device code provided by the attacker.
- Once authentication is completed, the attacker captures valid access and refresh tokens issued by the identity provider.
- The phishing infrastructure is fully automated, allowing operators to quickly generate new campaigns and victim-specific lures.
- Stolen tokens grant direct access to cloud services without requiring usernames or passwords.
- The service includes tooling to refresh tokens, extending access persistence even after the initial compromise.
- Access gained through tokens can enable mailbox access without triggering traditional login alerts.
- The campaign supports follow-on abuse, including email visibility and manipulation commonly associated with business email compromise.
- Infrastructure and workflows are designed to reduce reliance on malware delivery or exploit usage.
- The attack model focuses on social engineering users into completing legitimate authentication steps on attacker-controlled prompts.

Recommendations

- Review and restrict device code authentication flows where not operationally required.
- Monitor cloud authentication logs for unusual or unexpected device code sign-in activity.
- Enforce conditional access policies to reduce token usability from unknown or unmanaged devices.

- Educate users on phishing techniques that request completion of authentication steps outside normal workflows.
- Regularly audit cloud access tokens and revoke sessions associated with suspicious authentication patterns.

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
Qilin Ransomware EDR Killer Infection Chain Targets Security Controls	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an infection chain associated with the Qilin ransomware operation that includes a specialized component designed to disable endpoint detection and response tools. The activity demonstrates a structured sequence where threat actors deploy tooling to terminate security processes before launching ransomware, increasing the likelihood of successful impact.

This campaign may impact organizations in the financial sector that rely on endpoint security controls for ransomware defense. Organizations in the financial sector should be aware that attacks incorporating EDR-disabling components could affect detection, response, and recovery capabilities during intrusion activity.

Technical Details

- The infection chain begins after attackers already have interactive access to the target environment, rather than through an initial exploitation event.
- Threat actors deploy a dedicated binary commonly referred to as an “EDR killer”, designed specifically to interfere with endpoint security software.
- The tool enumerates running processes to identify security and monitoring products active on the system.
- Targeted security processes are deliberately terminated to reduce visibility before ransomware execution.
- The EDR killer relies on legitimate Windows functionality rather than exploiting kernel-level vulnerabilities.
- Process termination is performed methodically to ensure defensive controls are disabled before proceeding.
- Once security tooling is neutralized, attackers deploy ransomware with a reduced risk of detection or interruption.
- The infection chain reflects deliberate preparation and testing rather than opportunistic ransomware deployment.

- The tooling is lightweight and focused, indicating a specific operational role within the broader attack workflow.
- This approach highlights an increasing emphasis on defense evasion as part of ransomware operations.

Recommendations

- Monitor endpoints for suspicious process enumeration and termination activity, particularly involving security tooling.
- Restrict administrative access and closely audit accounts capable of stopping or modifying endpoint protection services.
- Implement tamper protection and self-defense features available within endpoint security platforms.
- Correlate endpoint events with identity and privilege usage to detect pre-ransomware preparation stages.
- Ensure incident response plans account for scenarios where endpoint visibility may be partially degraded.

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
Cookie-Controlled PHP Webshell Tradecraft Targets Linux Hosting Environments	**MEDIUM**	**CLEAR**	**Campaign**	**Open Source**

Executive Summary

Researchers have identified a stealthy post-compromise technique where attackers deploy PHP-based web shell on Linux servers that rely on HTTP cookies to control execution. Instead of exposing malicious behavior through visible request parameters, the web shells remain inactive during normal activity and activate only when specific attacker-supplied cookie values are present.

This campaign may impact organizations in the financial sector that operate Linux-based web applications or hosting environments. Organizations in the financial sector should be aware that cookie-controlled execution can reduce visibility in standard monitoring and logging workflows, potentially allowing persistent access to compromised servers to go undetected.

Technical Details

- The web shells use HTTP cookies as the primary control mechanism for malicious execution.
- Malicious PHP code remains dormant unless specific cookie values are provided in incoming requests.
- Cookie values are accessed at runtime using native PHP functionality, allowing attacker input to be consumed without additional parsing.
- Execution control is shifted away from URL parameters or request bodies to blend into normal web traffic.
- The activity has been observed across web requests, scheduled tasks, and trusted background workers.

- Multiple PHP implementations were identified, all sharing the same cookie-gated execution model.
- Some variants include layered obfuscation to reconstruct functions and payloads only after cookie validation.
- Persistence is achieved through scheduled tasks that recreate the web shell if it is removed.

Recommendations

- Monitor Linux servers for unexpected PHP scripts that reference cookie values during execution.
- Audit scheduled tasks for unauthorized jobs that recreate files in web-accessible directories.
- Restrict web server and PHP worker processes from spawning shell interpreters.
- Apply strong access controls and multi-factor authentication for hosting and administration panels.
- Increase visibility into HTTP cookie usage for anomalous or non-standard behavior.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Cookie-Controlled PHP Webshell Tradecraft Targets Linux Hosting Environments.

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Fake Installer Campaign Delivers Multi-Tool Monero Mining	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a long-running financially motivated campaign that distributes malware through fake software installers, abusing trust in legitimate software and services by luring victims into initiating downloads or execution as part of broader social-engineering workflows. This activity leads to the deployment of remote access tools and Monero cryptocurrency miners and follows a consistent, multi-stage infection chain that has evolved over time while retaining shared tooling and infrastructure, a pattern consistent with large-scale socially engineered delivery operations.

This campaign may impact organizations in the financial sector that allow software installation on user endpoints, as compromised systems could affect workstation performance, security visibility, and internal access. Organizations in the financial sector should be aware that long-running mining operations can coexist with other malicious tooling and increase the risk of extended unauthorized access.

Technical Details

- The infection chain begins with victims downloading what appears to be a legitimate software installer.
- Recent campaign variants use ISO files containing a malicious loader and a text file acting as a social engineering lure.
- The lure instructs users to bypass built-in security warnings, allowing the malicious loader to execute.

- The loader is heavily packed using multiple obfuscation layers to hinder analysis and detection.
- Once executed, the loader launches scripts that prepare the system for additional payload deployment.
- Depending on the campaign version, the operation deploys remote access tools, crypto miners, or both.
- A custom Monero mining component is used to download mining configurations and run invisibly in the background.
- Mining components include logic to reduce detection, such as stopping activity when analysis tools are running.
- Additional tools act as watchdogs, restoring mining activity or payloads if components are removed.
- Monetization extends beyond Cryptomining, with victims redirected to fake registration pages used for CPA fraud.

Recommendations

- Restrict execution of installer files from untrusted sources, including ISO-based installers.
- Educate users on social engineering techniques that prompt security bypass actions.
- Monitor endpoints for unexpected Cryptomining activity, resource consumption, and persistence mechanisms.
- Enforce application control policies to limit unauthorized loaders and scripting engines.
- Review systems for signs of long-term unauthorized tooling that may coexist with mining activity.

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
Actively Exploited Use-After-Free Vulnerability Patched in Google Chrome	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Google has disclosed a high-severity vulnerability in the Chrome desktop browser, tracked as CVE-2026-3910, which has been addressed in the latest stable update. The flaw originates from an inappropriate implementation within the V8 JavaScript engine, and Google has confirmed that exploitation is occurring in the wild.

This vulnerability may impact organizations in the financial sector that rely on Google Chrome for day-to-day business operations, as exploitation could affect endpoint security and user activity. Organizations in the financial sector should be aware that delayed patching of widely used browsers could affect user workstations and increase exposure to web-based attack vectors.

Technical Details

- The vulnerability addressed is a high-severity use-after-free flaw in the Dawn graphics component of Google Chrome. Improper memory management can allow memory corruption when handling crafted web content.
- The issue stems from an inappropriate implementation within V8 that can result in unintended browser behavior when processing crafted JavaScript content.
- Successful exploitation allows attackers to deliver malicious web content that triggers abnormal behavior during JavaScript execution.
- The vulnerability affects Chrome desktop platforms, including Windows, macOS, and Linux systems.
- Google has confirmed that this vulnerability is actively exploited in the wild at the time of disclosure.
- The affected component, V8, is responsible for executing JavaScript and WebAssembly content within the browser.
- Exploitation does not require local access and can be triggered through web-based interaction with malicious content.

Recommendations

- Update to the latest versions of Google Chrome for Windows/Linux: 146.0.7680.75 and for macOS:146.0.7680.76

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Command Execution Vulnerability in Cisco Smart Software Manager On-Prem	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Cisco has disclosed a critical vulnerability (CVE-2026-20160) affecting Cisco Smart Software Manager On-Prem (SSM On-Prem) that allows unauthenticated remote attackers to execute arbitrary commands. The issue arises from exposure of an internal service that enables interaction with a vulnerable API endpoint, potentially granting root-level access upon exploitation.

This vulnerability may impact organizations in the financial sector that rely on Cisco SSM On-Prem for license management and infrastructure operations. Organizations in the financial sector should be aware that unauthenticated command execution could affect system integrity, availability, and overall operational stability if affected instances remain unpatched.

Technical Details

- CVE-2026-20160 is a critical vulnerability affecting Cisco Smart Software Manager On-Prem deployments.
- The vulnerability is caused by exposure of an internal service to an external attack surface.
- A vulnerable API endpoint allows unauthenticated remote attackers to interact with the service.
- Successful exploitation enables execution of arbitrary commands on the underlying system.
- Commands are executed with root-level privileges, allowing full system control.
- The vulnerability is classified under CWE-668, indicating exposure of a resource to the wrong trust sphere.
- The vulnerability carries a CVSS v3.1 score of 9.8, reflecting critical severity.
- Exploitation does not require user interaction or prior authentication.
- Impact includes potential full system compromise, data manipulation, and service disruption.

Recommendations

- Upgrade Cisco Smart Software Manager On-Prem to version 9-202601 or later immediately.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Microsoft Fixes Critical Azure Kubernetes Service Vulnerability Without Customer Action	**HIGH**	**CLEAR**	**Vulnerability**	**Open Source**

Executive Summary

Microsoft has addressed a critical security vulnerability tracked as CVE-2026-33105 affecting Azure Kubernetes Service (AKS). The flaw was remediated on the service side by Microsoft, and customers are not required to take any action to apply the fix.

This vulnerability may impact organizations in the financial sector that operate containerized workloads on AKS. Organizations in the financial sector should be aware that while no customer-side remediation is required, understanding managed service vulnerabilities remains important for risk awareness and cloud governance.

Technical Details

- CVE-2026-33105 is a critical vulnerability affecting Azure Kubernetes Service.
- The issue exists within the managed AKS service rather than customer-managed components.
- Microsoft classified the vulnerability as critical based on its potential impact.

- The vulnerability was addressed directly by Microsoft through service-side remediation.

Recommendations

- No immediate action is required for customers using Azure Kubernetes Service.
- Continue monitoring cloud security advisories for managed service vulnerabilities.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Remote Code Execution Vulnerability in Kali Forms WordPress Plugin	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Kali Forms, a WordPress contact form and drag-and-drop builder plugin, contains a critical remote code execution vulnerability affecting versions 2.4.9 and earlier. The flaw allows unauthenticated attackers to execute arbitrary PHP code by abusing how the plugin processes user-supplied input during form handling.

This vulnerability may impact organizations in the financial sector that rely on WordPress-based websites for customer interaction, marketing, or informational services. Organizations in the financial sector should be aware that successful exploitation could affect website integrity, expose sensitive data, and disrupt public-facing services if vulnerable plugin versions are in use.

Technical Details

- CVE-2026-3584 is a critical remote code execution vulnerability affecting the Kali Forms WordPress plugin.
- The vulnerability carries a CVSS v3.1 score of 9.8, reflecting critical severity.
- The issue impacts Kali Forms versions 2.4.9 and earlier and is resolved in version 2.4.10 and later.
- The vulnerability is caused by improper control over code generation within the plugin's form processing logic.
- The *"prepare_post_data"* function improperly handles user-supplied input during form submission.
- User-controlled keys are directly mapped into internal placeholder storage without sufficient validation.
- These placeholders are later executed using the *"call_user_func"* function.
- This behavior allows attackers to inject and execute arbitrary PHP functions remotely.
- Exploitation does not require authentication, significantly increasing exposure for internet-facing sites.

Recommendations

- Upgrade the Kali Forms plugin immediately to version 2.4.10 or later.
- Disable the plugin if immediate patching is not possible.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Actively Exploited Authentication Bypass Vulnerability in FortiClient EMS	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Fortinet has identified a critical vulnerability in FortiClient Endpoint Management Server (EMS) that is actively exploited in the wild. The flaw allows unauthenticated attackers to bypass API authentication and authorization controls, potentially enabling remote code execution on affected systems.

This vulnerability may impact organizations in the financial sector that use FortiClient EMS for endpoint management and security operations. Organizations in the financial sector should be aware that unauthenticated access combined with command execution capabilities could affect system confidentiality, integrity, and availability if mitigations are not applied promptly.

Technical Details

- CVE-2026-35616 is a critical vulnerability affecting FortiClient EMS.
- The vulnerability has a CVSS score of 9.1, reflecting critical severity.
- The vulnerability is caused by improper enforcement of access controls within the FortiClient EMS API.
- Certain API requests fail to correctly validate authentication and authorization.
- Unauthenticated attackers can send specially crafted API requests to bypass security checks.
- Successful exploitation enables unauthorized execution of commands or code on the EMS server.
- Commands may be executed with high privileges, potentially leading to full system compromise.
- The vulnerability is classified under CWE-284, indicating improper access control.
- Fortinet has confirmed that exploitation is actively occurring in the wild.

Recommendations

- Apply the official hotfix for FortiClient EMS versions 7.4.5 and 7.4.6 immediately.
- Upgrade to FortiClient EMS version 7.4.7 or later when available to ensure a permanent fix.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Cisco Releases Security Updates Addressing Multiple Vulnerabilities	MEDIUM	CLEAR	Vulnerability	CSC

Executive Summary

Cisco has released security updates to remediate multiple vulnerabilities affecting its enterprise networking and management products. The addressed issues span improper authorization, privilege escalation, remote code execution, denial of service, and web-based attack vectors, with potential impact on confidentiality, integrity, and availability.

These vulnerabilities may impact organizations in the financial sector that rely on Cisco infrastructure and management platforms. Organizations in the financial sector should be aware that unpatched Cisco components could affect core network operations, management systems, and access to sensitive data.

Technical Details

- Cisco identified multiple high- and medium-severity vulnerabilities across networking and management products.
- High-severity issues include improper authorization and privilege escalation weaknesses in enterprise management platforms.
- Remote code execution and command injection vulnerabilities were identified in Cisco Integrated Management Controller components.
- Denial of service conditions were addressed in Cisco IOS XE Software.
- File handling weaknesses, including arbitrary file write risks, affect Cisco Nexus Dashboard Insights.
- Server-side request forgery vulnerabilities were identified in Cisco Nexus Dashboard and related management components.
- Unauthorized access issues were found in configuration backup REST APIs.
- Cross-site scripting vulnerabilities impact Cisco Integrated Management Controller web interfaces.
- Successful exploitation can enable attackers to gain elevated privileges, execute arbitrary commands, disrupt services, or access sensitive data.

Recommendations

- Review all Cisco products in use to determine exposure to the listed vulnerabilities.
- Apply the relevant security updates, mitigations, or workarounds provided by Cisco.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Drift Protocol Suffers USD 285 Million Loss in North Korea-Linked Cyber Heist	HIGH	CLEAR	Cyber Breach	Open Source

Executive Summary

Drift Protocol, a decentralized perpetual futures exchange operating on the Solana blockchain, suffered a major cyber breach resulting in the theft of approximately USD 285 million in user assets. The incident was confirmed to have occurred on April 1, 2026, and investigations link the operation to North Korean threat actors based on on-chain behavior and tradecraft patterns.

This breach may impact organizations in the financial sector that engage with decentralized finance platforms or blockchain-based trading services. Organizations in the financial sector should be aware that attacks combining social engineering, governance abuse, and blockchain transaction manipulation could affect digital asset exposure and operational risk.

Technical Details

- Attackers drained approximately USD 285 million in user assets from Drift Protocol within roughly 12 minutes.
- The breach did not exploit a smart contract coding flaw but relied on abuse of governance and administrative mechanisms.
- On-chain staging activity began on March 11, nearly three weeks before the execution of the heist.
- Attackers used durable nonce accounts on Solana to pre-sign transactions that could be executed later without expiring.
- Social engineering was used to trick multisig Security Council signers into pre-approving transactions with hidden administrative permissions.
- A governance migration to a 2-of-5 multisig threshold with zero timelock removed the protocol's final safeguard.
- The attackers created a fictitious token, CarbonVote Token (CVT), and manipulated trading activity to make it appear as legitimate collateral.
- Drift's price system mispriced a fake token, enabling withdrawal of real funds.
- Stolen funds were rapidly bridged from Solana to Ethereum within hours of the attack.
- Researchers believe the activity matches known North Korean cybercrime tactics.

Recommendations

- Review exposure to decentralized finance platforms and associated governance mechanisms.
- Implement governance change delays to allow detection of suspicious proposals.
- Monitor blockchain interactions for anomalous token creation and price manipulation activity.

- Conduct risk assessments for third-party DeFi platform usage and digital asset custody models.

Reference to the Source

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

Cookie-Controlled PHP Webshell Tradecraft Targets Linux Hosting Environments

Tactic	Technique	Description
Initial Access	T1190 Exploit Public-Facing Application	Attackers gain access through exposed web applications or hosting environments and use that access to introduce server-side tooling that blends into the web stack.
Persistence	T1505.003 Server Software Component: Web Shell	A PHP web shell is placed in a web-accessible location and designed to remain dormant during normal traffic, enabling long-term access through web requests.
Defense Evasion	T1027 Obfuscated/Encrypted File or Information	Payloads and scripts are obfuscated or encoded (for example, high-entropy strings and base64-encoded blobs) to reduce inspection and evade simple content-based detections.
Defense Evasion	T1140 Deobfuscate/Decode Files or Information	Attackers decode inline payloads at runtime, such as echo <blob> | base64 -d > <file> to reconstruct PHP content on disk with minimal interactive footprint.
Command and Control	T1105 Ingress Tool Transfer	Additional files or second-stage scripts are retrieved using file ingress utilities such as curl or wget, often writing directly into web directories or application paths.
Execution	T1059.004 Command and Scripting Interpreter: Unix Shell	Web-facing workloads (for example, php-fpm, apache2, nginx) spawn shell interpreters (sh, bash, dash) to execute attacker-provided commands from webshell logic or injected requests.
Persistence	T1053.003 Scheduled Task/Job: Cron	Persistence is established via cron, including jobs created by hosting tooling (for example, cPanel) and recurring execution patterns (including short intervals such as one-minute loops).
Defense Evasion	T1222.002 File and Directory Permissions Modification	File or directory permissions are modified to enable write/execute access in web paths or to ensure persistence artifacts remain accessible to the compromised runtime context.

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	Recipients may share TLP:AMBER+STRICT information only with members of their own

	acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	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
Administrative Key	A highly privileged cryptographic key used to control system or platform settings.
Authentication	The process of verifying a user or system's identity before granting access.
Authentication Bypass	A security weakness that allows attackers to gain access without valid credentials.
Authorization	A control that determines what actions an authenticated user or system is allowed to perform.
Azure Kubernetes Service (AKS)	A managed cloud platform for running containerized applications.
BEC	Business Email Compromise
Blockchain	A distributed ledger technology that records transactions across multiple systems.
Browser Vulnerability	A security flaw affecting internet browsers that can be triggered by viewing malicious web content.
Cloud Service	A computing service delivered over the internet rather than hosted on local infrastructure.

Code Injection	A vulnerability that allows attackers to insert and execute malicious code.
Compromised Credentials	Usernames or passwords that have been stolen or misused by attackers.
Containerized Workload	Applications packaged in containers for consistent deployment across environments.
Cookie-Controlled Execution	A stealth technique where malicious code activates only when specific cookies are present.
CPA	Cost Per Action
Critical Severity	A classification indicating a vulnerability can lead to full system compromise with minimal effort.
Cron Job	A scheduled task in Linux systems that runs automatically at set intervals.
Cross-Chain Bridging	Moving digital assets between different blockchain networks.
CSC	UAE Cyber Security Council
CVE	Common Vulnerabilities and Exposures – a unique identifier assigned to publicly disclosed security vulnerabilities.
CVSS	Common Vulnerability Scoring System – a method for measuring the severity of security vulnerabilities.
CWE	Common Weakness Enumeration – a classification system for software security flaws.
Decentralized Finance (DeFi)	Financial services built on blockchain technology without a centralized authority.
Destructive Attack	A cyberattack intended to disable systems or data rather than generate financial gain.
Digital Assets	Assets such as cryptocurrencies or tokens stored and transferred electronically.
Durable Nonce	A blockchain feature allowing transactions to be pre-signed and executed later.
Endpoint	Any device such as a laptop, server or workstation connected to a network.
Endpoint Detection and Response (EDR)	A security solution that detects and responds to threats on user devices and servers.
Endpoint Management	A centralized system used to manage, secure and monitor user devices.
Governance Abuse	Manipulation of administrative or approval mechanisms to gain unauthorized control.
Hotfix	A rapid update released to address an urgent security issue
HTTP Cookie	Data stored by a browser that is sent with web requests to maintain session state.
Improper Access Control	A weakness where systems fail to correctly restrict access to sensitive functions or data.
Insider Trust Abuse	Exploiting legitimate access or trusted relationships to carry out attacks.
Lateral Movement	An attacker technique used to spread from one system to others within a network.
Linux Hosting Environment	A server environment running the Linux operating system, often used for web applications.

Managed Infrastructure	Enterprise systems maintained centrally rather than by individual users.
Managed Service	A system fully maintained and patched by a service provider rather than the customer.
Multisignature (Multisig)	A control requiring multiple approvals before performing sensitive actions.
Network Segmentation	The practice of dividing networks into isolated sections to limit attack spread.
North Korea–Linked Threat Actor	An attacker group associated with North Korean state-sponsored cyber operations.
Obfuscation	A technique used to hide malicious code to avoid detection.
Operational Disruption	Interruption of normal business operations caused by system outages or data loss.
Oracle	A service that provides external data, such as prices, to blockchain systems.
Patch Management	The process of applying updates to fix vulnerabilities.
Persistence	A method attackers use to maintain long-term access to compromised systems.
Phishing	A social engineering technique that tricks users into opening malicious links or attachments.
PHP Web shell	A malicious script placed on a web server that allows attackers to control the system remotely.
Privilege Escalation	An attack technique where attackers gain higher access rights than intended.
Public-Facing Application	A system or website accessible from the internet.
Remote Code Execution (RCE)	A security flaw that allows attackers to run commands or programs remotely on a target system.
Self-Healing Mechanism	Malware behaviour that automatically restores itself after removal.
Smart Contract	Self-executing code on a blockchain that controls transactions automatically.
Social Engineering	Manipulating people into performing actions or revealing information.
Threat Actor	A malicious individual or group conducting cyber operations.
Token Manipulation	Artificially influencing the perceived value of a digital asset.
MENA Region	Geographic regions referenced in threat activity impacting organizations operating there.
Use-After-Free	A memory management error where software uses memory that has already been released.
V8 Engine	The JavaScript execution engine used by Google Chrome to process web content.
VPN	Virtual Private Network – a secure remote connection into an internal network.
Web shell	A backdoor tool that enables attackers to execute commands through a web interface.
Web-Based Attack	An attack delivered through websites or internet-facing applications.

Wiper Malware	Malicious software designed to permanently destroy data and render systems unusable rather than stealing information or demanding payment.
WordPress Plugin	An add-on component used to extend the functionality of WordPress websites.