TLP:CLEAR

ADGM THREAT INTELLIGENCE NEWSLETTER

PREPARED BY ADGM CTI

CATEGORY	ACTIONABLE
AUDIENCE	ADGM FSRA ENTITIES
DATE	30/4/2026
OVERALL THREAT SCORE	ELEVATED
TARGET SECTOR	FINANCIAL SERVICES
TARGET REGION	MENA & GLOBAL
ATTRIBUTION	MULTIPLE
TLP	CLEAR

TLP:CLEAR

WEEKLY SUMMARY REPORT – 30 April 2026

9	7	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 broad set of threat activity and security weaknesses affecting enterprise technology, with a noticeable concentration on supply-chain abuse, perimeter infrastructure compromise and exploitation of trusted platforms. The entries cover active malware campaigns leveraging collaboration tools, developer ecosystems, mobile apps and network appliances, alongside confirmed data breaches at major financial institutions through a third-party vendor. From a financial sector perspective, these developments may impact operational resilience, data protection, and trust in third-party dependencies. Organisations should prioritise patching, strengthen vendor risk management, monitor for abuse of legitimate tools and ensure legacy or end-of-life systems are decommissioned to reduce exposure to persistent and evolving threats.

ADGM THREAT INTELLIGENCE SUMMARY

DinDoor Campaign Abusing Deno Runtime via Malicious MSI Installers [Campaign] [High]

New NGate Campaign Hides in a Trojanized NFC Payment Application [Campaign] [High]

UAT-4356 Deploys FIRESTARTER Malware Against Cisco Firepower Appliances [Campaign] [High]

FakeWallet Campaign Spreads Crypto-Stealing Malware via iOS App Store [Campaign] [High]

Mustang Panda Deploys New LOTUSLITE Variant Targeting Banking and Policy-Focused Entities [Campaign] [High]

Self-Propagating Supply Chain Worm Hijacks npm Packages to Steal Developer Tokens [Campaign] [Medium]

Bitwarden CLI Compromise Linked to Ongoing Supply Chain Campaign [Campaign] [Medium]

UNC6692 Uses Social Engineering via Microsoft Teams to Deploy Custom Malware [Campaign] [Medium]

Jasper Sleet Campaign Exploits Remote Hiring to Gain Trusted Cloud Access [Campaign] [Medium]

Actively Exploited Command Injection Vulnerability in D-Link Routers [Vulnerability] [High]

High-severity Vulnerability in Juniper Networks Junos OS and Junos OS Evolved [Vulnerability] [High]

Oracle April 2026 Critical Patch Update Addresses Multiple High-Risk Vulnerabilities [Vulnerability] [High]

Multiple Critical and High-Severity Vulnerabilities in Atlassian Data Center and Server Products [Vulnerability] [High]

Critical Privilege Escalation Vulnerability in ASP.NET Core Data Protection [Vulnerability] [High]

Critical Path Traversal Vulnerability in LogScale Self-Hosted Deployments [Vulnerability] [Medium]

Multiple Security Vulnerabilities Addressed in GitLab CE and EE Updates [Vulnerability] [Medium]

Citizens Bank and Frost Bank Confirm Third-Party Data Breach Linked to Everest Ransomware [Cyber Breach] [High]

Name	Threat Severity Rating	TLP	Attribution	Originating Source
DinDoor Campaign Abusing Deno Runtime via Malicious MSI Installers	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an ongoing malware campaign, tracked as DinDoor. The malware is delivered to victims through phishing or drive-by downloads using Microsoft installer (MSI) files and downloads the Deno runtime from the legitimate project endpoint, that delivers a backdoor using deceptive Microsoft installer (MSI) files and the legitimate Deno JavaScript runtime on Windows systems. The campaign abuses trusted installer workflows and signed runtimes to run obfuscated JavaScript payloads while keeping visible artifacts and user prompts to a minimum.

This campaign may impact organizations in the financial sector where MSI execution and developer runtimes are permitted by default. Banks, fintech platforms and virtual asset environments should be aware that such abuse of legitimate tools could affect endpoint visibility and enable persistent unauthorized access without triggering traditional alerts.

Technical Details

- The campaign is distributed through malicious MSI installer files that appear as legitimate business documents or software, relying on user execution to start the infection chain.
- When launched, the MSI uses standard installation mechanisms to silently execute embedded scripts while suppressing user-visible errors or prompts.
- As part of execution, the malware checks whether the Deno runtime is already present on the system and installs it if missing, without requiring administrator privileges.
- Deno is then used to run attacker-controlled JavaScript, shifting execution away from traditional compiled binaries and blending into normal runtime activity.
- The JavaScript payload is obfuscated and can be written briefly to disk or passed directly to Deno in encoded form for in-memory execution.
- Once running, the backdoor generates a unique fingerprint based on host attributes, allowing the operator to track individual infected systems.
- The malware validates outbound connectivity before establishing regular communication with its command infrastructure.
- The malware checks in every second and if it fails it handles the error, switches to another C2 server, and tries again, providing the attacker with ongoing remote access.
- Some variants embed campaign metadata directly in remote request paths, enabling shared backend infrastructure across multiple operations.
- Differences observed between samples indicate a modular framework that allows operators to change execution behavior while keeping the same core logic.

Recommendations

- Restrict execution of MSI installers to trusted sources and approved user groups through application control policies.
- Monitor endpoints for unexpected installation or execution of developer runtimes such as Deno in non-development environments.
- Enhance detection coverage for script execution chains spawned from installer processes.
- Review network activity for repeated short-interval outbound requests following installer execution.
- Reinforce user awareness around unsolicited installer files posing as documents or routine business software.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – DinDoor Campaign Abusing Deno Runtime via Malicious MSI Installers

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 NGate Campaign Hides in a Trojanized NFC Payment Application	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a new variant of the NGate malware family that is distributed through a trojanized Android NFC (Near Field Communication) payment application. The attackers exploited the legitimate 'HandyPay' application by modifying an NFC relay application, inserting AI-generated malicious code that captures card PINs without requesting extra permissions.

This campaign may impact organizations in the financial sector by enabling payment card abuse and unauthorized cash withdrawals through compromised mobile devices. Financial institutions and payment service environments should be aware that NFC-based fraud delivered via trusted-looking mobile apps could affect customer payment security and transaction monitoring controls.

Technical Details

- The campaign relies on trojanizing a legitimate Android application, HandyPay, which is designed to relay NFC card data between paired devices.
- Threat actors patch the original app with malicious code while retaining its normal NFC relay functionality to avoid arousing suspicion.
- Distribution occurs through websites impersonating lottery and fake Google Play page, requiring users to manually install the app outside official stores.

- Once installed, the app prompts the user to set it as the default NFC payment application, a behavior that is consistent with the legitimate version.
- No additional Android permissions are requested, allowing the malware to operate with minimal user visibility.
- Victims are prompted to enter their payment card PIN and scan their card using NFC on the infected device.
- The trojanized app forwards NFC card data to an attacker-controlled device, enabling contactless payments and ATM withdrawals.
- Payment card PINs are separately exfiltrated to a remote command server over HTTP, outside of the app's normal infrastructure.
- The operator's receiving device is tied to an email address hardcoded in the malicious app, ensuring exclusive control of relayed data.
- Analysis indicates similarities across samples, suggesting a coordinated campaign targeting Android users.

Recommendations

- Advise customers and employees to install mobile applications only from official app stores.
- Monitor for patterns of NFC-related payment fraud that align with mobile device compromise.
- Strengthen detection of unauthorized contactless withdrawals and anomalous card usage.
- Review mobile security controls to identify sideloaded applications acting as payment handlers.
- Enhance awareness programs around fake payment protection or lottery applications targeting mobile users.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – New NGate Campaign Hides in a Trojanized NFC Payment Application

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
UAT-4356 Deploys FIRESTARTER Malware Against Cisco Firepower Appliances	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers examined a malware campaign attributed to the UAT-4356 threat actor, where the FIRESTARTER backdoor is deployed by exploiting critical flaws in Cisco Firepower and Secure Firewall devices running ASA (Adaptive Security Appliance) or FTD (Firepower Threat Defense) software. The attackers gain root access,

implant malicious hooks into the LINA (*Linux Native*) packet-processing engine, and maintain persistent remote control of the devices even after the vulnerabilities are patched.

This campaign may impact organizations in the financial sector that operate network edge firewalls as part of critical infrastructure. Institutions should be aware that compromised perimeter devices could affect network integrity, credential security, and long-term trust in security appliances if persistence remains undetected.

Technical Details

- The campaign targets Cisco Firepower and Secure Firewall devices exposed to the internet, focusing on systems running ASA or FTD software.
- Initial access is assessed to have occurred through exploitation of vulnerabilities CVE-2025-20333 and/or CVE-2025-20362 before patches were applied.
- After exploitation, attackers deployed FIRESTARTER as a Linux ELF backdoor designed to run directly on affected firewall appliances.
- FIRESTARTER enables remote access and command execution, functioning as a long-term command-and-control mechanism.
- The malware persists through firmware updates and standard reboots, allowing attackers to regain access without re-exploitation.
- Persistence is achieved by modifying system configuration files and reinstalling itself when termination signals or shutdown events occur.
- FIRESTARTER installs a hook into the LINA process, Cisco's core network inspection engine, enabling execution of attacker-provided shellcode.
- The malware cleans up artifacts by restoring file timestamps, suppressing error output, and deleting temporary files to reduce visibility.
- Victim identification is performed through inspection of WebVPN requests containing specific XML elements, triggering additional payload stages.
- In observed incidents, FIRESTARTER was used alongside LINE VIPER, which enabled unauthorized VPN sessions and access to device credentials.

Recommendations

- Immediately assess exposed firewall appliances for signs of persistent compromise.
- Reimage affected devices using fixed software releases rather than relying on upgrades alone.
- Treat existing device configurations, credentials, and certificates as untrusted until regenerated.
- Review historical exposure to vulnerable VPN services on firewall infrastructure.
- Strengthen monitoring for anomalous behavior originating from network security appliances.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – UAT-4356 Deploys FIRESTARTER Malware Against Cisco Firepower Appliances

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
FakeWallet Campaign Spreads Crypto-Stealing Malware via iOS App Store	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an ongoing campaign, tracked as FakeWallet, involving phishing iOS applications published in the Apple App Store that masquerade as legitimate cryptocurrency wallets. These apps redirect users to malicious installation flows and deploy trojanized wallet applications designed to steal recovery phrases and sensitive wallet data.

This campaign may impact organizations in the financial sector offering digital asset services or supporting cryptocurrency users. Institutions should be aware that trusted mobile app ecosystems could be abused to facilitate crypto theft, potentially affecting customer assets, confidence, and fraud response processes.

Technical Details

- The campaign involves phishing apps published in the Apple App Store that impersonate popular cryptocurrency wallets using similar names and icons.
- Many of the apps appear benign at first, functioning as simple utilities or placeholders to pass review and avoid suspicion.
- Upon launch, the apps redirect users to external browser pages posing as official sources for unavailable wallet apps.
- These pages guide users through installing trojanized wallet applications using provisioning profiles outside normal App Store protections.
- Malicious modules are embedded into modified wallet apps through injected libraries or direct source code changes.
- The malware targets wallet recovery flows, intercepting seed phrases entered by users during wallet creation or restoration.
- Stolen recovery phrases are encrypted using RSA algorithm followed by Base64 encoding and exfiltrated to attacker-controlled servers.
- Some variants display phishing prompts within the app interface, closely mimicking legitimate security or verification dialogs.
- Both hot wallets and cold wallet companion apps are targeted, with tailored logic for each wallet type.

Recommendations

- Advise users and employees to install cryptocurrency applications only from verified publishers and official sources.

- Monitor for reports of mobile wallet compromise tied to phishing or unexpected in-app verification prompts.
- Strengthen customer awareness programs around recovery phrase protection and social engineering risks.
- Review mobile threat intelligence for abuse of provisioning profiles and sideloaded wallet applications.
- Incorporate mobile app ecosystem threats into digital asset risk assessments and fraud monitoring workflows.

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
Mustang Panda Deploys New LOTUSLITE Variant Targeting Banking and Policy-Focused Entities	HIGH	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a new campaign attributed to Mustang Panda that deploys an updated LOTUSLITE backdoor variant through targeted delivery mechanisms. The activity uses spear-phishing lures and DLL sideloading with legitimate, signed executables to execute the backdoor while blending into normal system activity.

This campaign may impact organizations in the financial sector, particularly institutions operating in or connected to regional banking ecosystems. Financial services organizations should be aware that focused targeting using banking-themed lures and trusted execution paths could affect endpoint security and long-term access within sensitive environments.

Technical Details

- The campaign delivers LOTUSLITE via spear-phishing messages containing malicious CHM (Compiled HTML) files themed around support or banking-related requests.
- When opened, the CHM displays a benign prompt and triggers embedded HTML that downloads and executes a malicious JavaScript loader.
- The JavaScript extracts a legitimate Microsoft-signed executable alongside a malicious DLL to a local directory.
- Execution relies on DLL sideloading, where the signed executable loads the attacker-supplied LOTUSLITE DLL without validating its source.

- The updated backdoor, tracked as LOTUSLITE v1.1, introduces a modular design with new exported functions and campaign-specific naming.
- Command-and-control traffic is sent over HTTPS using hardcoded dynamic DNS domains, allowing the malware to blend into normal network traffic.
- The implant supports remote command execution, file operations, and session management through custom packet-based communication.
- Code changes include updated packet magic values and runtime API resolution to reduce static detection opportunities.
- Persistence is maintained using registry autorun mechanisms, now isolated into dedicated functions for flexibility and evasion.
- Artefacts within the malware indicate overlapping victim themes, linking banking-focused activity with earlier campaigns targeting policy and geopolitical entities.

Recommendations

- Monitor email entry points for spear-phishing attempts carrying CHM or archive-based attachments.
- Restrict or disable unnecessary execution of CHM files and script-based loaders on endpoints.
- Detect DLL sideloading behavior involving signed executables loading unexpected libraries.
- Enhance endpoint monitoring for unusual API resolution and encrypted outbound beaconing patterns.
- Review security awareness programs to address banking-themed lures and support-style social engineering.

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
Self-Propagating Supply Chain Worm Hijacks npm Packages to Steal Developer Tokens	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified an ongoing supply-chain campaign in which attackers compromised legitimate npm packages and introduced a self-propagating malware, often referred to as a canister-backed worm. The malicious code executes automatically during package installation, steals credentials from developer environments, and attempts to spread by abusing compromised publishing access.

This campaign may impact organizations in the financial sector that depend on software development pipelines, internal tooling, or open-source components. Financial institutions should be aware that exposure

within developer or CI/CD environments could affect cloud credentials, source-code systems, and downstream applications built using tainted packages.

Technical Details

- The campaign affected legitimate npm packages, including developer tooling and utilities, by replacing package contents with malicious install-time logic.
- The malware executes during installation using post-install hooks, allowing it to run without additional user interaction.
- Once executed, the malware scans the host environment for sensitive credentials and secrets commonly used by developers and build systems.
- Collected data includes environment variables, configuration files, and credentials associated with package registries, cloud services, and CI/CD platforms.
- Stolen information is exfiltrated off-host using remote endpoints, blending into normal outbound network traffic.
- The malware encrypts collected data when possible before transmission, indicating an intent to evade detection and analysis.
- In addition to credential theft, the payload contains logic designed to identify whether the infected environment can publish packages.
- If publishing access is available, the malware attempts to inject itself into other packages and republish them, enabling automated spread.
- The campaign uses infrastructure hosted via canister-based services as part of its command-and-control and data-handling workflow.
- Analysis shows strong similarities across affected packages, suggesting a coordinated effort rather than isolated malicious uploads.

Recommendations

- Identify and remove affected npm package versions from developer workstations and CI/CD environments.
- Rotate credentials and tokens that may have been exposed on systems where compromised packages were installed.
- Review package publishing history and access controls for signs of unauthorized publishing activity.
- Monitor build and development environments for unexpected install-time script execution.
- Strengthen controls around dependency management, including validation of package integrity before use.

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
Bitwarden CLI Compromise Linked to Ongoing Supply Chain Campaign	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers uncovered a supply chain attack in which the Bitwarden CLI (Command Line Interface), an open-source password manager was distributed with malicious code. Attackers abused a trusted automation workflow to insert a backdoor during the build process, allowing the compromised package to be published without disrupting normal CI/CD operations. The technique aligns with methods observed in other repositories affected by the same campaign.

This campaign may impact organizations in the financial sector that rely on CLI tools in development and automation pipelines. Institutions should be aware that compromise of widely used tooling could affect CI/CD environments, expose sensitive credentials, and introduce risk across interconnected cloud and development systems.

Technical Details

- The campaign involved a compromised version of the Bitwarden CLI package published through the standard package distribution channel.
- Attackers abused a trusted automation workflow in the project's build pipeline to introduce a malicious JavaScript file into the package contents.
- The injected file acted as a loader for additional malicious components while allowing the CLI to continue functioning normally.
- Malicious logic focused on harvesting credentials and sensitive configuration data from affected environments.
- The code attempted to extract tokens and secrets associated with source control, cloud services, and build automation systems.
- Stolen data was exfiltrated using outbound connections triggered during normal CLI execution.
- The malware contained logic to propagate further by targeting writable projects and automation workflows.
- Execution occurred in developer systems and CI runners, increasing the potential blast radius beyond a single endpoint.
- The compromise was limited to the CLI package and did not affect other distribution channels or products.
- The campaign is assessed as part of a broader, ongoing supply chain activity leveraging similar build-pipeline abuse patterns.

Recommendations

- Identify and remove the affected CLI package version from development systems and build environments.
- Rotate credentials that may have been exposed within affected CI/CD pipelines or developer machines.

- Review build logs and automation workflows for unauthorized changes or unexpected executions.
- Monitor for unusual package publishing activity or unexpected outbound connections during build processes.
- Strengthen controls around build automation, including tighter permissions and validation of automated workflows.

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
UNC6692 Uses Social Engineering via Microsoft Teams to Deploy Custom Malware	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a multi-stage intrusion campaign attributed to UNC6692, where attackers use persistent social engineering through Microsoft Teams to gain an initial foothold. The activity involves impersonating IT helpdesk personnel and tricking users into installing malicious components under the guide of email remediation.

This campaign may impact organizations in the financial sector that rely on Microsoft Teams and cloud-based collaboration platforms. Institutions should be aware that trusted user interactions during incident-like scenarios could allow attackers to establish long-term access using valid credentials and custom malware.

Technical Details

- The campaign begins with a large-scale email flood designed to overwhelm users and create urgency prior to direct engagement.
- Attackers then contact victims via Microsoft Teams, posing as internal helpdesk staff offering assistance with the email disruption.
- Victims are directed to click a link claiming to install a local patch, which opens a web page hosted on attacker-controlled infrastructure.
- The page delivers an AutoHotKey executable and script that automatically executes upon download, initiating reconnaissance activity.
- This execution installs a malicious browser extension, later used as the primary persistence mechanism.
- Persistence is reinforced through startup shortcuts and scheduled tasks that ensure the extension is continuously active.
- Additional malware components are downloaded, including tools used to tunnel network traffic and execute commands remotely.

- The threat actor conducts internal network scanning and enumerates local administrator accounts.
- Administrative access is leveraged to dump sensitive process memory and extract credential material.
- Using harvested credentials, the attackers move laterally to domain controllers and exfiltrate directory and registry data.

Recommendations

- Implement heightened monitoring for Microsoft Teams messages originating from external or newly created accounts.
- Review installer and script execution activity initiated through collaboration platforms.
- Apply additional scrutiny to newly scheduled tasks and browser extensions on user endpoints.
- Monitor for abnormal credential usage and rapid lateral movement following user interaction events.
- Reinforce user awareness around unsolicited technical support requests delivered through chat platforms.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – UNC6692 Uses Social Engineering via Microsoft Teams to Deploy Custom Malware

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

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Jasper Sleet Campaign Exploits Remote Hiring to Gain Trusted Cloud Access	MEDIUM	CLEAR	Campaign	Open Source

Executive Summary

Researchers have identified a campaign attributed to Jasper Sleet, where threat actors exploit remote hiring and digital onboarding processes to infiltrate organizations as fraudulent IT workers. The activity leverages stolen or fabricated identities to progress through recruitment, onboarding, and payroll setup, resulting in the creation of legitimate user account.

This campaign may impact organizations in the financial sector that rely on remote hiring and cloud-based HR platforms. Institutions operating large SaaS environments should be aware that trusted access gained through onboarding workflows could affect internal data exposure, cloud applications, and identity governance controls.

Technical Details

- The campaign begins with reconnaissance of external career portals to identify open technical roles and understand recruitment workflows used by target organizations.

- Threat actors programmatically access recruiting application interfaces exposed via external job portals to browse roles and submit applications at scale.
- Multiple external accounts are used in consistent patterns to access recruitment APIs, distinguishing the activity from normal job-seeking behavior.
- Applications are tailored using information extracted from job descriptions, enhancing the likelihood of passing initial screening stages.
- During recruitment, attackers communicate with hiring teams using standard email and conferencing platforms to complete interviews.
- Once hired, legitimate accounts are provisioned as part of standard onboarding, including payroll and tax information setup.
- Sign-ins to newly created HR accounts originate from infrastructure previously associated with the campaign.
- After onboarding, the actors access internal SaaS applications such as collaboration, email, and document platforms using valid credentials.
- Early post-hire activity often shows anomalies such as access from multiple locations and use of anonymous or proxy infrastructure.
- Repeated location-based sign-in irregularities indicate remote access techniques inconsistent with normal employee behavior.

Recommendations

- Monitor recruitment systems for repetitive or automated access patterns originating from external user accounts.
- Review onboarding and payroll changes performed by newly created employee accounts, especially soon after hire.
- Strengthen identity monitoring for new employees, including anomaly detection related to location and access behavior.
- Correlate communications activity during recruitment with identity and access telemetry to surface inconsistencies early.
- Incorporate threat awareness into hiring processes to help identify suspicious candidate behavior during remote recruitment.

For a detailed breakdown of tactics, techniques, and procedures (TTPs), refer to the Annexure – Jasper Sleet Campaign Exploits Remote Hiring to Gain Trusted Cloud Access

Reference to the Source

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Actively Exploited Command Injection Vulnerability in D-Link Routers	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

D-Link has disclosed a critical command injection vulnerability, tracked as CVE-2025-29635, affecting DIR-823X series routers running specific firmware versions. The flaw is being actively exploited in the wild via remote HTTP POST requests, allowing unauthenticated attackers to execute arbitrary commands and deploy Mirai botnet variants.

This vulnerability may impact organizations in the financial sector that still rely on legacy or unmanaged network infrastructure. Institutions should be aware that compromised edge devices could be abused for DDoS activity and persistent footholds, potentially affecting network availability and downstream services.

Technical Details

- CVE-2025-29635 is a command injection vulnerability that allows attackers to send crafted HTTP POST requests to the affected router.
- The flaw does not effectively enforce authentication, enabling remote exploitation without valid credentials.
- Impacted devices include D-Link DIR-823X series routers running firmware versions 240126 and 24082.
- These devices have been officially designated as end-of-life as of September 2025, and no security patches are available.
- Threat actors are actively exploiting the vulnerability to execute system-level commands on the router.
- Successful exploitation enables installation of Mirai botnet variants on the compromised device.
- Once infected, the router can participate in large-scale distributed denial-of-service attacks.
- The compromise also allows attackers to maintain persistent access to the affected device.
- Exploited devices may generate outbound traffic to untrusted external hosts and unusual network ports.
- The active exploitation indicates continued interest in leveraging unpatched, internet-exposed infrastructure.

Recommendations

- Decommission affected devices by replacing all D-Link DIR-823X routers, as no patches are available due to end-of-life status.
- Block known malicious IP addresses at the network perimeter to limit follow-on abuse from compromised devices.
- Monitor outbound network traffic for unusual connections to unknown external hosts or high ports.

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

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
High-severity Vulnerability in Juniper Networks Junos OS and Junos OS Evolved	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Juniper Networks has disclosed a high-severity vulnerability, tracked as CVE-2026-33797, affecting Junos OS and Junos OS Evolved. The flaw stems from improper input validation and allows an unauthenticated attacker on an adjacent network to reset established BGP sessions using specially crafted but valid BGP packets.

This vulnerability may impact organizations in the financial sector that rely on stable BGP routing for connectivity with service providers, partners, or internal networks. Institutions operating affected Junos versions should be aware that sustained exploitation could affect routing stability and availability of critical network services.

Technical Details

- CVE-2026-33797 is caused by improper input validation within the BGP implementation of Junos OS and Junos OS Evolved.
- An unauthenticated attacker with adjacent network access can exploit the flaw without needing valid credentials.
- The attack uses specially crafted, yet protocol-compliant BGP packets sent within an already established session.
- Successful exploitation forces the targeted BGP session to reset, resulting in a Denial-of-Service condition.
- Both external BGP (eBGP) and internal BGP (iBGP) sessions are affected by this behavior.
- The vulnerability impacts deployments using either IPv4 or IPv6 networking environments.
- Repeated exploitation can continuously disrupt BGP sessions, leading to prolonged routing instability.
- Affected Junos OS versions include 25.2 releases prior to 25.2R2.
- Affected Junos OS Evolved versions include 25.2-EVO releases prior to 25.2R2-EVO.

Recommendations

- Upgrade affected systems to fixed versions: Junos OS 25.2R2, 25.4R1, or later.
- For Junos OS Evolved, update to 25.2R2-EVO, 25.4R1-EVO, or later releases.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Oracle April 2026 Critical Patch Update Addresses Multiple High-Risk Vulnerabilities	HIGH	CLEAR	Vulnerability	CSC

Executive Summary

Oracle has released its April 2026 Critical Patch Update (CPU), addressing 481 security vulnerabilities across 28 Oracle product families. A significant portion of these vulnerabilities are classified as high to critical severity, with several allowing remote code execution and unauthenticated exploitation over the network.

These vulnerabilities may impact organizations in the financial sector that depend on Oracle middleware, databases, ERP platforms, and financial services applications. Institutions should be aware that delayed remediation could affect system availability, data integrity, and the security of internet-facing and transaction-critical environments.

Technical Details

- The April 2026 CPU resolves a total of 481 vulnerabilities, with approximately 78% originating from third-party components.
- Affected products span 28 families, indicating a broad exposure across Oracle enterprise software ecosystems.
- Oracle Communications is the most impacted product line, accounting for 139 vulnerabilities, including 93 that are exploitable without authentication.
- Several Oracle Communications issues are rated critical, with CVSS scores reaching 9.8 and enabling remote code execution.
- Oracle Financial Services Applications received 75 patches, with 59 vulnerabilities exploitable without credentials.
- Critical issues in financial services products allow remote code execution and pose risks to financial data and transaction systems.
- Oracle Fusion Middleware includes 59 patched vulnerabilities, 46 of which are unauthenticated, some with CVSS scores of 9.8.
- Exploitation of middleware flaws could enable broad access across interconnected enterprise applications.
- Oracle MySQL received 34 fixes, including a critical vulnerability in MySQL Enterprise Backup that allows remote code execution.
- The Oracle Database ecosystem was updated with 27 patches across components such as GoldenGate, REST Data Services, and TimesTen, with maximum CVSS scores up to 7.5.

Recommendations

- Apply the April 2026 Critical Patch Update across all affected Oracle products without delay.
- Prioritize patching of internet-facing systems and externally exposed services.

- Expedite remediation for Oracle Communications, Fusion Middleware, and Financial Services Applications deployments.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Critical and High-Severity Vulnerabilities in Atlassian Data Center and Server Products	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Atlassian has released its April 2026 security updates addressing multiple critical and high-severity vulnerabilities affecting Bamboo, Bitbucket, Confluence, Jira Software, and Jira Service Management Data Center and Server products. The vulnerabilities span remote code execution, command injection, information disclosure, request smuggling, cross-site scripting, and denial-of-service conditions, many originating from third-party dependencies.

These vulnerabilities may impact organizations in the financial sector that rely on Atlassian platforms for development workflows, service management, and internal collaboration. Institutions should be aware that unpatched systems could affect service availability, expose sensitive data, or allow unauthorized access within enterprise environments.

Technical Details

- The April 2026 updates address both critical- and high-severity issues across multiple Atlassian Data Center and Server products.
- A critical OS command injection vulnerability (CVE-2026-21571) affects Bamboo Data Center and could lead to remote code execution.
- Several products, including Confluence, Jira Software, and Jira Service Management, are affected by a remote code execution issue in org.yaml:snakeyaml (CVE-2022-1471).
- Mutation cross-site scripting vulnerabilities in dompurify (CVE-2024-47875) affect Jira Software and Jira Service Management.
- Denial-of-service vulnerabilities impact multiple platforms through dependencies such as brace-expansion, axios, netty, and json-smart.
- Man-in-the-middle vulnerabilities are present in Jira Service Management and Jira Software due to affected okhttp and xmlhttprequest components.
- Confluence Data Center and Server are impacted by multiple file inclusion and path traversal vulnerabilities in node-tar.

- HTTP request smuggling issues affect Bamboo and Confluence through Apache Tomcat and Netty dependencies.
- Improper authorisation vulnerabilities in commons-beanutils affect Jira Software and Jira Service Management.
- The majority of vulnerabilities stem from third-party libraries embedded within Atlassian products.

Recommendations

- Update all affected Atlassian Data Center and Server products to the fixed or latest versions released by Atlassian.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Privilege Escalation Vulnerability in ASP.NET Core Data Protection	**HIGH**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

Microsoft has released out-of-band security updates to address a critical privilege escalation vulnerability, tracked as CVE-2026-40372, affecting ASP.NET Core. The issue arises from improper cryptographic signature validation within the Data Protection component, enabling attackers to escalate privileges to SYSTEM level under certain conditions.

This vulnerability may impact organizations in the financial sector running ASP.NET Core applications that rely on Data Protection for authentication or token handling. Financial institutions should be aware that exploitation could affect application trust boundaries, potentially allowing continued access even after patching if remediation steps are incomplete.

Technical Details

- CVE-2026-40372 is rated critical with a CVSS score of 9.1 and impacts the ASP.NET Core Data Protection component distributed via NuGet.
- The vulnerability is caused by improper validation of cryptographic signatures used to protect sensitive authentication material.
- Affected versions include Microsoft.AspNetCore.DataProtection from v10.0.0 through v10.0.6.
- An attacker who can interact with a vulnerable application may be able to forge authentication tokens.
- Successful exploitation enables privilege escalation to SYSTEM level within the affected application context.
- Forged tokens could be used to bypass authentication and gain unauthorized access to protected resources.

- Exploitation may allow attackers to access or disclose sensitive application data.
- The issue can also enable persistence, as previously issued tokens remain valid unless explicitly invalidated.
- Patching alone does not invalidate tokens generated during the vulnerable period, requiring additional remediation.

Recommendations

- Upgrade Microsoft.AspNetCore.DataProtection to version 10.0.7 or later across all affected applications.
- Rotate the ASP.NET Core Data Protection key ring to invalidate previously issued cryptographic tokens.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Critical Path Traversal Vulnerability in LogScale Self-Hosted Deployments	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

LogScale has disclosed a critical path traversal vulnerability, tracked as CVE-2026-40050, affecting specific self-hosted versions of the platform. The flaw allows unauthenticated remote attackers to exploit improper path handling and access sensitive files on the underlying server.

This vulnerability may impact organisations in the financial sector operating self-hosted logging and SIEM infrastructure. Institutions should be aware that exposure of internal files could affect log integrity, system credentials, and operational visibility if vulnerable deployments remain unpatched.

Technical Details

- CVE-2026-40050 is an unauthenticated path traversal vulnerability with a CVSS v3.1 score of 9.8, indicating critical severity.
- The issue affects only self-hosted LogScale deployments and does not impact SaaS or next-generation SIEM offerings.
- Exploitation does not require valid credentials, increasing the risk for internet-accessible instances.
- A vulnerable application improperly restricts file path access, allowing crafted requests to traverse outside intended directories.
- Successful exploitation may enable attackers to read sensitive files from the server file system.
- Exposed files could include configuration data, credentials, or other operational artifacts depending on deployment setup.
- Affected general availability versions range from 1.224.0 through 1.234.0.

- Impacted long-term support versions include 1.228.0 and 1.228.1.
- The vulnerability does not require chaining with other flaws to achieve file disclosure.
- Fixed releases introduce proper path validation to prevent access beyond permitted file locations.

Recommendations

- Upgrade vulnerable self-hosted LogScale deployments to a patched version immediately.
- Apply one of the fixed versions: 1.235.1 or later, 1.234.1 or later, 1.233.1 or later, or 1.228.2 (LTS).

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Multiple Security Vulnerabilities Addressed in GitLab CE and EE Updates	**MEDIUM**	**CLEAR**	**Vulnerability**	**CSC**

Executive Summary

GitLab has released security updates addressing multiple vulnerabilities across GitLab Community Edition (CE) and Enterprise Edition (EE). The vulnerabilities include cross-site request forgery, cross-site scripting, denial-of-service conditions, and access control weaknesses that affect core components such as the GraphQL API, Web IDE, and import functionality.

These vulnerabilities may impact organizations in the financial sector that rely on GitLab for source code management, CI/CD pipelines, and collaboration. Institutions should be aware that unpatched instances could allow unauthorized actions, service disruption, or exposure of sensitive project data within development environments.

Technical Details

- GitLab identified several high-severity vulnerabilities affecting both CE and EE deployments across multiple versions.
- CVE-2026-4922 exposes a CSRF flaw in the GraphQL API, potentially allowing attackers to trigger unauthorized actions via crafted requests.
- CVE-2026-5816 impacts the Web IDE through improper path validation, creating conditions for unintended file access.
- A cross-site scripting issue in Storybook (CVE-2026-5262) could enable execution of malicious scripts in user browsers.
- Multiple denial-of-service vulnerabilities affect components such as discussion threads, notes endpoints, Jira imports, and the GraphQL API.
- These DoS issues could allow attackers to exhaust system resources and disrupt GitLab availability.

- CVE-2026-6515 highlights insufficient session expiration controls for virtual registry credentials, increasing exposure risk if credentials are misused.
- Improper access control vulnerabilities affect issue description rendering and project fork relationship APIs.
- Lower-severity issues include weaknesses in the Mermaid sandbox and API authorization logic.
- GitLab addressed all reported issues in coordinated updates across supported release branches.

Recommendations

- Upgrade GitLab Community Edition and Enterprise Edition instances to the fixed versions immediately.
- Apply version 18.11.1, 18.10.4, or 18.9.6 depending on the deployed release branch.

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

back to top

Name	Threat Severity Rating	TLP	Attribution	Originating Source
Citizens Bank and Frost Bank Confirm Third-Party Data Breach Linked to Everest Ransomware	**HIGH**	**CLEAR**	**Cyber Breach**	**Open Source**

Executive Summary

Citizens Bank and Frost Bank, two major financial institutions in the United States, have confirmed a data breach following claims by the Everest ransomware group, which listed both banks on its extortion leak site in April 2026. The attackers released sample datasets and issued a time-bound ultimatum, while both banks stated the incident originated from a compromised third-party service provider rather than direct intrusion into their internal networks.

This breach may impact organizations in the financial sector that rely on external vendors for data processing or storage. Financial institutions should be aware that third-party breaches could affect customer information exposure, fraud risks, and response obligations even when core banking systems remain uncompromised.

Technical Details

- The Everest ransomware group added Citizens Financial Group and Frost Bank to its dark web leak site on April 20, 2026, using a double-extortion model to pressure victims.
- Attackers claimed to have stolen approximately 250,000 customer records from Frost Bank, including sensitive financial and personal data such as Social Security numbers and tax identifiers.
- For Citizens Bank, the group alleged access to roughly 3.4 million records from a SQL database dump, primarily containing names, addresses, account numbers, and internal document flags.
- Analysis of released samples indicated that Citizens Bank data did not include Social Security or tax identification numbers.
- Both banks confirmed the breach stemmed from unauthorized access to a third-party vendor's systems.

- Citizens Bank stated that most of the exposed data was masked test data, with only a limited set of real customer information involved.
- Frost Bank reported engaging external cybersecurity experts and noted the incident may be related to recent cybercriminal claims.
- The attackers released redacted samples as proof and threatened full disclosure if demands were not met within the stated deadline.

Recommendations

- Review and strengthen third-party risk management and vendor security oversight processes.
- Monitor for signs of fraud, phishing, or scams potentially leveraging exposed customer information.
- Coordinate incident response efforts with affected vendors and external security specialists.
- Communicate proactively with impacted customers using trusted and verified channels.
- Incorporate third-party breach scenarios into financial sector incident response and resilience planning.

Reference to the Source

back to top

Appendix A - Tactics, Techniques & Procedures (TTPs)

DinDoor Campaign Abusing Deno Runtime via Malicious MSI Installers

Tactics	Techniques	Description
Initial Access	User Execution	MSI lures are designed to be executed by the victim, initiating the chain via a deceptive installer.
Execution	Command and Scripting Interpreter	PowerShell and VBScript are used to launch and stage the runtime and payload execution.
Execution	Signed Binary Proxy Execution	Windows Installer execution is leveraged to run installer logic as the initial execution vector.
Defense Evasion	Obfuscated/Compressed Information	JavaScript is delivered in base64 form, and one variant is additionally obfuscated to hinder static analysis.
Defense Evasion	Trusted Developer Utilities Proxy Execution	The legitimate Deno runtime is installed/used to run attacker-controlled JavaScript, complicating monitoring where Deno is not covered.
Defense Evasion	Hidden Window	Script execution is launched with hidden window settings to reduce user visibility.
Discovery	System Information Discovery	The payload derives a unique host identifier using system attributes (e.g., username/host characteristics/memory/OS details).
Discovery	Peripheral Device Discovery	GPU enumeration is performed prior to additional tasking, consistent with environment vetting.
Command and Control	Application Layer Protocol	The backdoor communicates over HTTP-based requests and polls periodically, with retry and rotation behavior.
Command and Control	Non-Standard Port / Local Port Binding (behavioral)	The payload binds a local listener as a single-instance control to avoid reinfection/duplicate execution

New NGate Campaign Hides in a Trojanized NFC Payment Application

Tactic	Techniques	Description
Initial Access	T1660 - Phishing	NGate has been distributed using dedicated websites.
Credential Access	T1417.002 - Input Capture: GUI Input Capture	NGate tries to obtain victims' PIN codes via a patched text box.
Exfiltration	T1646 - Exfiltration Over C2 Channel	NGate exfiltrates victims' PINs over HTTP.

UAT-4356 Deploys FIRESTARTER Malware Against Cisco Firepower Appliances

Tactic	Techniques	Description
Initial Access	T1190 - Exploit Public-Facing Application	The APT actors gained access to the victim's Cisco Firepower device, likely by exploiting CVE-2025-20333 and/or CVE-2025-20362.
Execution	T1059 - Command and Scripting Interpreter	FIRESTARTER uses a special function to run shell commands that create /opt/cisco/config/platform/rmdb/CSP_MOUNT_LIST if it is missing. FIRESTARTER runs callback commands to manage its files.
Persistence	T1543 -Create or Modify System Process	FIRESTARTER invokes mprotect to enable execution of newly injected code.

	T1546.004 -Event Triggered Execution: Unix Shell Configuration Modification	FIRESTARTER registers a callback function that is automatically triggered when the program receives any of the following termination-related signals: SIGTERM, SIGINT, SIGQUIT, SIGABRT, SIGHUP, or SIGTSTP.
	T1547 -Boot or Logon Autostart Execution	Persistence is maintained by modifying a boot-time configuration/mount script so FIRESTARTER runs on startup.
	T1133 -External Remote Services	The APT actors used LINE VIPER to establish illegitimate VPN sessions.
	T1078 -Valid Accounts	The APT actors used valid user accounts for their illegitimate VPN sessions (the user accounts belonged to former employees
Defense Evasion	T1222 - File and Directory Permissions Modification	FIRESTARTER creates the /opt/cisco/platform/logs/var/log/ directory with full read/write/execute permissions. FIRESTARTER uses chown and chmod to modify file permissions.
	T1564 - Hide Artifacts: Hidden Users	FIRESTARTER redirects standard error (stderr) messages to /dev/null and hides them from the console.
	T1070.004 - Indicator Removal on Host: File Deletion	FIRESTARTER deletes the following files: CSP_MOUNT_LIST, CSP_MOUNT_LIST.tmp, and /usr/bin/lina_cs.
	T1070.006 - Indicator Removal on Host: Timestomp	FIRESTARTER uses touch -r to copy timestamps from original files to modified and temporary ones, explicitly to match the original.
	T1036.005 - Masquerading: Match Legitimate Resource Name or Location	FIRESTARTER accesses its own binary located at /usr/bin/lina_cs on the victim device.
	T1055 - Process Injection	FIRESTARTER injects shellcode into a library's code section before the start of the text segment.
Discovery	T1057 - Process Discovery	FIRESTARTER enumerates LINA's virtual memory map to locate the private read-write (rw-p) segment associated with lina.
	T1082 - System Information Discovery	The APT actors used LINE VIPER to access Cisco Firepower device configuration elements, including administrative credentials, certificates, and private keys
Command and Control	T1219 - Remote Access Tools	FIRESTARTER is a Linux ELF designed to execute on Cisco Firepower and Secure Firewall devices, serving as a C2 channel for remote access and control.

UNC6692 Uses Social Engineering via Microsoft Teams to Deploy Custom Malware

Tactic	Techniques	Description
Initial Access	Phishing via service	Social engineering through enterprise collaboration messages impersonating helpdesk support, following an email "noise" event to increase urgency.
	User Execution	Victim prompted to click through a "patch/utility" workflow and interact with on-screen buttons that initiate staging.
Credential Access	Credential Phishing	Web-based credential prompt using a repeated-entry trick to capture validated credentials and reduce typos.
Execution	Command and Scripting Interpreter	Use of scripting and Python tooling to perform scanning, tunneling, and local command execution.

Persistence	Scheduled Task/Job	Scheduled tasks used to ensure the malicious extension is loaded and to manage headless browser processes.
	Startup Items	Startup execution used to verify the extension is running and to re-establish execution if needed.
	Browser Extensions	Malicious Chromium-based extension installed outside official extension distribution channels and maintained via browser registration mechanisms.
Discovery	Network Service Discovery	Internal scanning for common management/remote access services prior to lateral movement.
Lateral Movement	Remote Services	Remote execution and remote desktop activity to move from an initial host to additional servers.
Credential Access	OS Credential Dumping	Memory extraction from the security authority process to obtain credential material.
Lateral Movement	Use of Authentication Material	Use of password hashes to authenticate and move laterally to domain controllers.
Command and Control	Proxy/Tunneling	WebSocket-based tunneling and SOCKS-style proxying to route traffic through the compromised host.
Collection	Screen Capture	Screen captures targeting in-focus windows associated with browsing and tool execution on privileged systems.
	Data from Directory	Collection of directory database material and related system/registry artifacts from domain controllers.
Exfiltration	Exfiltration over web service / cloud storage	Upload of stolen credentials/metadata via cloud object storage workflows used as attacker infrastructure.
	Exfiltration via third-party service	Use of a consumer file-sharing application to move credential-dump and collected data out of the environment.

Jasper Sleet Campaign Exploits Remote Hiring to Gain Trusted Cloud Access

Tactic	Techniques	Description
Resource Development	Acquire Infrastructure	Researching job postings and recruitment workflows using external-facing HR platforms
	Establish Accounts	Creation and use of external applicant accounts and later legitimate employee accounts
Initial Access	Valid Accounts	Logging in with newly created internal identities acquired through fraudulent hiring
Persistence	Account Manipulation	Updating payroll and onboarding details using legitimate HR system access
Defense Evasion	Use of Trusted Relationships	Blending malicious activity within normal HR, onboarding, and employee behavior.

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
APT	Advanced Persistent Threat: A highly organised threat group that maintains long-term, covert access to target organisations.
ASA	Adaptive Security Appliance: A network firewall device used to protect organisational perimeter networks.
ASP.NET Core	A Microsoft framework used to build and run enterprise web applications and services.
Authentication Bypass	A weakness that allows attackers to access systems without valid user credentials.
Backdoor	Malicious functionality that enables attackers to re-enter a system after initial compromise.
Bamboo	An enterprise automation and build tool used in software development pipelines.
BGP	Border Gateway Protocol: A core internet routing protocol that controls how data moves between networks.
Blockchain Platform	Enterprise systems that support blockchain-based transactions and digital assets.
Botnet	A collection of compromised devices controlled remotely by attackers.
CanisterWorm	A self-propagating malware that spreads through compromised software packages.
CHM File	A Windows help file format commonly abused to deliver malicious payloads.
CI/CD	Continuous Integration / Continuous Deployment: Automated systems used to build and deploy software.
CLI	Command Line Interface: A text-based method for interacting directly with systems or applications.
Command and Control (C2)	Infrastructure attackers use to manage and control compromised systems remotely.
Command Injection	A vulnerability allowing attackers to execute system commands using crafted input.

Confluence	An enterprise collaboration and internal documentation platform.
Critical Patch Update (CPU)	A scheduled release of security fixes addressing multiple vulnerabilities at once.
CSRF	Cross-Site Request Forgery: An attack that forces authenticated users to perform unintended actions.
CSC	UAE Cyber Security Counsil
CVE	Common Vulnerabilities and Exposures: A standardized identifier for publicly disclosed security flaws.
CVSS	Common Vulnerability Scoring System: A framework used to rate vulnerability severity.
Cyber Breach	An incident involving unauthorised access to systems or sensitive data.
DDoS	Distributed Denial-of-Service: An attack that disrupts services by overwhelming them with traffic.
Denial-of-Service (DoS)	An attack intended to disrupt system or service availability.
Deno Runtime	A JavaScript execution environment abused to run malicious scripts.
DIR-823X	A D-Link router model affected by an actively exploited vulnerability.
DLL Sideloading	A technique where attackers force legitimate software to load malicious files.
End-of-Life (EOL)	Hardware or software that is no longer supported or patched by the vendor.
Endpoint	An individual device such as a server, workstation, or network appliance.
Everest Ransomware	A ransomware group using data theft and extortion against organisations.
Financial Services Applications	Enterprise platforms used for banking, payments, and financial operations.
FIRESTARTER	A persistent backdoor malware targeting network firewall appliances.
Firewall	A system that filters and controls network traffic based on security rules.
Fusion Middleware	Oracle software used to connect and manage enterprise applications.
GitLab CE / EE	Source code and DevOps platforms used in development and automation pipelines.
HTTP Request Smuggling	An attack that exploits inconsistencies in how web servers process requests.
iBGP / eBGP	Internal / External BGP: Routing protocols used within or between organisations.
Infrastructure Compromise	Unauthorized access to core systems such as firewalls or routers.
Jira Service Management	A platform used for IT service management and workflows.
Jira Software	A platform used for project and issue tracking.
Key Ring	Secure storage used to protect cryptographic keys and tokens.
LINE VIPER	Malware used to establish unauthorized VPN access on network devices.
LogScale	A log management and security monitoring platform.
LOTUSLITE	A backdoor malware variant used in targeted espionage campaigns.
Malicious MSI	A manipulated installer file used to deliver malware.
Man-in-the-Middle (MITM)	An attack where communications are intercepted or altered in transit.
Mirai	Malware that hijacks internet-connected devices to build botnets.
MSI	Microsoft Installer file format used to install applications on Windows systems.
Mustang Panda	A state-aligned cyber espionage group conducting long-term campaigns.
MySQL	A database platform used to store and manage application data.
Network Appliance	Dedicated hardware used for networking or security functions.
npm	A software package ecosystem commonly used in application development.
Oracle Communications	Oracle products supporting network and communication services.
OS Command Injection	A vulnerability enabling execution of commands on the underlying system.

Out-of-Band Update	An emergency security fix released outside regular patch schedules.
Path Traversal	A flaw that allows attackers to access files outside intended directories.
Persistence	Techniques attackers use to maintain long-term access to systems.
Privilege Escalation	Gaining higher access rights than originally permitted.
Remote Code Execution (RCE)	A vulnerability allowing attackers to run arbitrary code remotely.
Router	A device that directs network traffic between different networks.
SaaS	Software as a Service: Applications delivered over the internet.
Secure Firewall	Enterprise-grade devices used to protect network perimeters.
Self-Hosted Deployment	Software installed and managed by the organisation rather than a cloud provider.
Supply Chain Attack	An attack that compromises trusted software, vendors, or services.
SYSTEM Account	The highest privilege level in Windows operating systems.
Third-Party Vendor Risk	Security risk introduced by external service providers.
Token Forgery	Creation of fraudulent authentication tokens to bypass controls.
UAT-4356	Threat actor identifier linked to persistent firewall intrusions.
Unauthenticated Access	Ability to exploit systems without logging in.
Virtual Asset	Digital assets such as cryptocurrencies or tokenized instruments.
WebVPN	Browser-based VPN access used on network appliances.
XSS	Cross-Site Scripting: A flaw allowing malicious scripts to run in user browsers.