Date of Publication
November 3, 2026

Hive Pro

Hiveforce Labs

MONTHLY

# THREAT DIGEST

## Vulnerabilities, Attacks, and Actors

OCTOBER 2026

# Table Of Contents


Summary..... 03

Insights..... 04

Threat Distribution..... 05

Celebrity Vulnerabilities..... 06

Vulnerabilities Summary..... 14

Attacks Summary..... 24

Adversaries Summary..... 28

Targeted Products..... 29

Targeted Countries..... 36

Targeted Industries..... 37

Top MITRE ATT&CK TTPs..... 38

Top Indicators of Compromise (IOCs)..... 39

Vulnerabilities Exploited..... 42

Attacks Executed..... 100

Adversaries in Action..... 120

MITRE ATT&CK TTPS..... 125

Top 5 Takeaways..... 136

Recommendations..... 137

Appendix..... 138

Indicators of Compromise (IoCs)..... 139

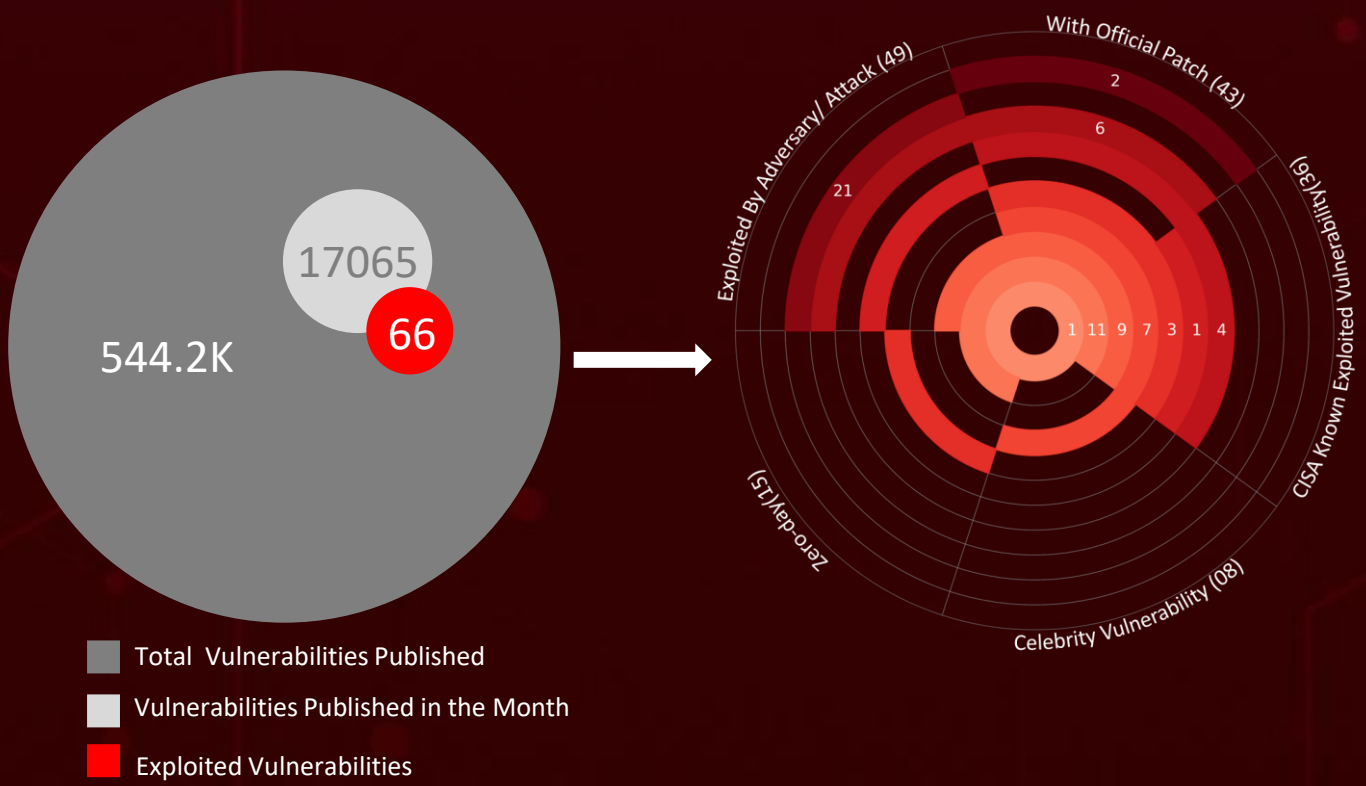
What Next?..... 145

# Summary

**October** reshaped the cybersecurity landscape, with **15 zero-day** vulnerabilities actively exploited. One of the most notable threats came from **Armory Castle** (UNC5221), a suspected China-nexus espionage group that exploited **CVE-2026-102764** in BeyondTrust Remote Support as a zero-day, exposing privileged credentials and downstream systems. Citrix also patched **CVE-2026-88779**, a NetScaler SAML zero-day that lets unauthenticated attackers crash appliances, plant web shells, and steal configuration backups.

Additionally, **PHP2Shell** (CVE-2026-109618 and CVE-2026-109619) puts nearly every PHP release since 5.4 at risk of unauthenticated remote code execution, with a group assessed to be Lazarus-linked already mapping 216 unpatched hosts. Attackers also hijacked the release process of **LiteLLM**, an AI gateway with about 23 million weekly downloads, to ship the privcollect stealer that harvests cloud, AI, and CI/CD secrets.

Moreover, the suspected nation-state cluster **CL-STA-0954** deployed the memory-resident PEERSTITCH implant after stealing configurations and keys for over 500 FortiGate firewalls from a telecom provider's FortiManager. Meanwhile, **SafePay ransomware** has hit at least 600 organizations, breaking in through stolen or brute-forced credentials and edge-device flaws before destroying backups and encrypting data. With risks like these growing, strong defensive measures are more important than ever.



# Insights

**In October 2026**, a geopolitical cybersecurity landscape unfolds, revealing **United Kingdom, United Arab Emirates, Australia, United States,** and **Iraq** as the top-targeted countries

Highlighted in **October 2026** is a cyber battleground encompassing the **Financial, Telecommunications, Aviation, IT Services,** and **Technology** sectors, designating them as the top industries

**Shai-Hulud** Hijacks Tensorlake's npm SDK and Wipes Home Directories When Stolen Tokens Are Revoked

**CVE-2026-73570** Fuels a Zimbra SNMP Exploitation Wave That Breached 274 Mail Servers

**PHP2Shell Flaws** Put Nearly Every PHP Release Since 5.4 at Risk of Unauthenticated Code Execution

Stolen Tokens Turn a **LiteLLM** Release into the privcollect Stealer Targeting Cloud and CI/CD Secrets

Suspected China-Nexus **Armory Castle** Exploits BeyondTrust Zero-Day CVE-2026-102764 for Espionage

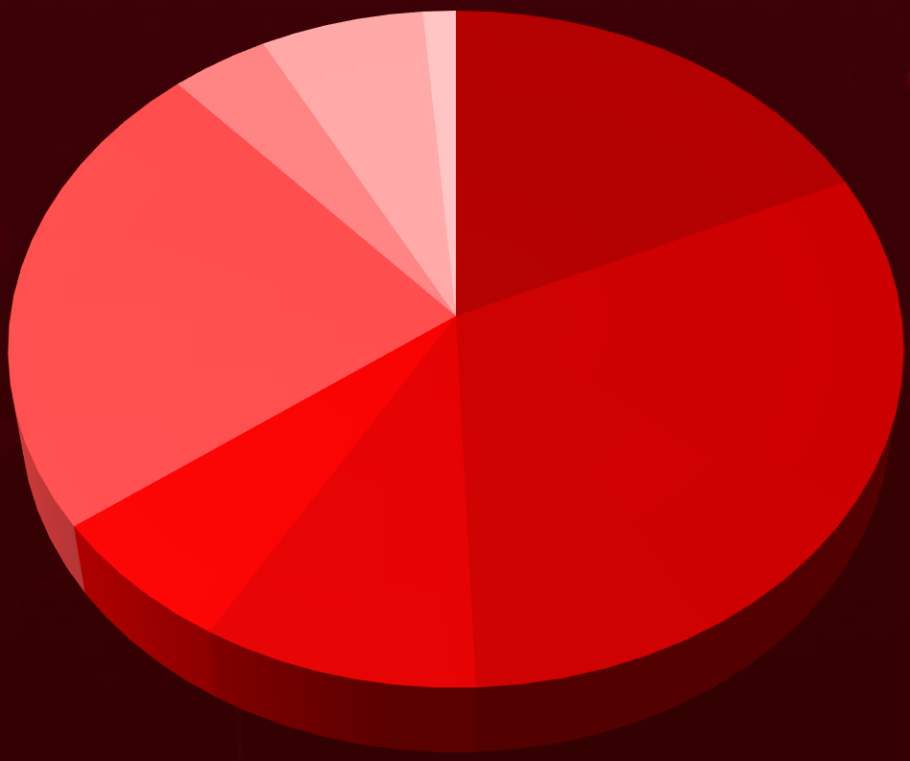
**CL-STA-0954** Hides PEERSTITCH Inside FortiOS After Stealing Keys for 500+ FortiGate Firewalls

**SafePay Ransomware** Surges Past 600 Victims Through Stolen Credentials and Edge-Device Flaws

North Korea's TraderTraitor Uses a Fake Terraform Add-On to Plant **FLATROOF** and **ROOFDECK** Backdoors

# Threat Distribution



# Celebrity Vulnerabilities

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-47575 | FortiJump | Fortinet FortiManager | CL-STA-0954 |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:fortinet:fortimanager:*:*:*:*:*:*:*:* | PEERSTITCH |
| Fortinet FortiManager Missing Authentication Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-306 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.fortiguard.com/psirt/FG-IR-24-423 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-109618 | PHP2Shell | PHP Group PHP (5.4 through 8.5.11) | Lazarus |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:php:php:*:*:*:*:*:*:*:* | - |
| PHP2Shell (PHP Out-of-Memory Corruption Vulnerability) |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-1325, CWE-416, CWE-755, CWE-824 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.php.net/archive/2026.php#2026-10-21-5 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-109619 | PHP2Shell | PHP Group PHP (5.4 through 8.5.11) | Lazarus |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:php:php:*:*:*:*:*:*:*:* | - |
| PHP2Shell (PHP Remote Code Execution Vulnerability) |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-1325, CWE-416, CWE-755, CWE-824 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.php.net/archive/2026.php#2026-10-21-5 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-111497 | Node2Shell | Node.js (22.x before 22.23.4, 24.x before 24.22.1, 26.x before 26.12.1, and End-of- Life versions), Bun (before 1.4.4), Google Brotli (1.0.3 through 1.2.0), and End-of Life versions), Python Brotli (before 1.2.1), brotlicffi (before 1.2.1.0), Microsoft .NET 8 (before 8.0.33), .NET 9 (before 9.0.22), .NET 10 (before 10.0.14), .NET 11 (before RC3) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:nodejs:nod, e.js:*:*:*:*:*:*:*:*, cpe:2.3:a:google:brotl, i:*:*:*:*:*:*:*:* | - |
| Node.js Brotli Decoder Out-of-Bounds Write Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINKS |
| | CWE-787, CWE-252 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://nodejs.org/en/blog/release/v22.23.4/, https://nodejs.org/en/blog/release/v24.22.1/, https://nodejs.org/en/blog/release/v26.12.1/, https://bun.com/blog/bun-v1.4.4, https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-111497, https://github.com/google/brotli/releases, https://pypi.org/project/Brotli/1.2.1/, https://pypi.org/project/brotlicffi/1.2.1.0/ |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-96652</td><td>Plex2Shell</td><td rowspan="2">Plex Media Server (Before 1.43.3.10861)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*</td><td rowspan="2">XMRig, myawesomeproxy</td></tr>
<tr><td rowspan="3">Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-918</td><td>T1190: Exploit Public-Facing Application</td><td>https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-96654 | Plex2Shell<br>ZERO-DAY | Plex Media Server (Before 1.43.3.10861) | - |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:* | XMRig, myawesomeproxy |
| Plex Media Server Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINKS |
| | CWE-84 | T1190: Exploit Public-Facing Application | https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/ |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-96655</td><td>Plex2Shell</td><td rowspan="2">Plex Media Server (Before 1.43.3.10861)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*</td><td rowspan="2">XMRig, myawesomeproxy</td></tr>
<tr><td rowspan="3">Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-918</td><td>T1190: Exploit Public-Facing Application, T1550.001: Application Access Token, T1105: Ingress Tool Transfer</td><td>https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-96656</td><td>Plex2Shell</td><td rowspan="2">Plex Media Server (Before 1.43.3.10861)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:*</td><td rowspan="2">XMRig, myawesomeproxy</td></tr>
<tr><td rowspan="3">Plex Media Server External Control of File Name or Path Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-73</td><td>T1190: Exploit Public-Facing Application, T1129: Shared Modules, T1574: Hijack Execution Flow</td><td>https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/</td></tr>
</table>

# Vulnerabilities Summary

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-73570 | Zimbra Collaboration Suite (ZCS) OS Command Injection Vulnerability | Synacor Zimbra Collaboration Suite (ZCS) | ✗ | ✓ | ✓ |
| CVE-2026-88779 | Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability | Citrix NetScaler ADC and NetScaler Gateway, Citrix NetScaler ADC - FIPS | ✓ | ✓ | ✓ |
| CVE-2026-104286 | Fortinet FortiMail Path Traversal Vulnerability | Fortinet FortiMail | ✓ | ✓ | ✓ |
| CVE-2026-21589 | Atlassian Multiple Products Arbitrary File Access Vulnerability | Atlassian Bitbucket Data Center Version, Confluence Data Center Version, Jira Service Management Data Center, Jira Software Data Center, Bamboo Data Center, Crowd Data Center, Crucible and Fisheye | ✗ | ✗ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2022-36553 | Hytec Inter HWL-2511-SS Command Injection Vulnerability | Hytec Inter HWL-2511-SS | ✗ | ✗ | ✗ |
| CVE-2025-34035 | EnGenius EnShare Cloud Service OS Command Injection Vulnerability | EnGenius EnShare Cloud Service | ✗ | ✗ | ✗ |
| CVE-2024-23625 | D-Link UPnP SUBSCRIBE Code Injection Vulnerability | D-Link DAP-1650 devices | ✗ | ✗ | ✗ |
| CVE-2021-35394 | Realtek Jungle SDK Remote Code Execution Vulnerability | Realtek Jungle SDK | ✗ | ✓ | ✓ |
| CVE-2023-1389 | TP-Link Archer AX-21 Command Injection Vulnerability | TP-Link Archer AX21 (AX1800) firmware | ✗ | ✓ | ✓ |
| CVE-2024-7029 | AVTECH AVM1203 Command Injection Vulnerability | AVTECH AVM1203 | ✗ | ✗ | ✗ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2024-10915 | D-Link Command Injection Vulnerability | D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028 | ✗ | ✗ | ✗ |
| CVE-2024-23624 | D-Link DAP-1650 Command Injection Vulnerability | D-Link DAP-1650 devices | ✗ | ✗ | ✗ |
| CVE-2019-17621 | D-Link DIR-859 Router Command Execution Vulnerability | D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01 | ✗ | ✓ | ✓ |
| CVE-2019-7256 | Nice Linear eMerge E3-Series OS Command Injection Vulnerability | Linear eMerge E3-Series devices | ✗ | ✓ | ✓ |
| CVE-2021-36380 | Sunhillo SureLine OS Command Injection Vulnerablity | Sunhillo SureLine | ✗ | ✓ | ✓ |
| CVE-2024-21887 | Ivanti Connect Secure and Policy Secure Command Injection Vulnerability | Ivanti Connect Secure and Ivanti Policy Secure | ✓ | ✓ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2023-46805 | Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability | Ivanti ICS 9.x, 22.x and Ivanti Policy Secure | ✓ | ✓ | ✓ |
| CVE-2024-46048 | Tenda exeCommand Command Injection Vulnerability | Tenda FH451 | ✗ | ✗ | ✗ |
| CVE-2024-35340 | Tenda exeCommand Command Injection Vulnerability | Tenda FH1206 | ✗ | ✗ | ✗ |
| CVE-2024-32314 | Tenda AC500 formexeCommand Command Injection Vulnerability | Tenda AC500 | ✗ | ✗ | ✗ |
| CVE-2024-32292 | Tenda exeCommand Command Injection Vulnerability | Tenda W30E v1.0 | ✗ | ✗ | ✗ |
| CVE-2024-32281 | Tenda exeCommand Command Injection Vulnerability | Tenda AC7V1.0 | ✗ | ✗ | ✗ |
| CVE-2022-35555 | Tenda W6 exeCommand Command Injection Vulnerability | Tenda W6 | ✗ | ✗ | ✗ |
| CVE-2022-26289 | Tenda exeCommand Command Injection Vulnerability | Tenda M3 1.10 | ✗ | ✗ | ✗ |
| CVE-2022-37055 | D-Link Routers Buffer Overflow Vulnerability | D-Link Routers | ✗ | ✓ | ✗ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2024-10914 | D-Link NAS Command Injection Vulnerability | D-Link Routers | ✗ | ✗ | ✗ |
| CVE-2026-36356 | MeiG Smart FORGE_SLT711 GoAhead Command Injection Vulnerability | MeiG Smart FORGE_SLT711 | ✗ | ✗ | ✗ |
| CVE-2025-67038 | Lantronix EDS5000 Code Injection Vulnerability | Lantronix EDS5000 | ✗ | ✓ | ✓ |
| CVE-2014-8361 | Realtek SDK Improper Input Validation Vulnerability | Realtek SDK | ✗ | ✓ | ✓ |
| CVE-2016-20016 | MVPower Remote Command Execution Vulnerability | MVPower CCTV DVR models | ✗ | ✗ | ✗ |
| CVE-2024-3721 | TBK DVR OS Command Injection Vulnerability | TBK DVR-4104 and DVR-4216 | ✗ | ✗ | ✗ |
| CVE-2025-34037 | Linksys E-Series Routers OS Command Injection Vulnerability | Linksys E-Series Routers | ✗ | ✗ | ✗ |
| CVE-2023-26801 | lb-link bl-lte300_firmware Command Injection Vulnerability | LB-LINK | ✗ | ✗ | ✗ |
| CVE-2023-41011 | China Mobile Intelligent Home Gateway Command Execution Vulnerability | China Mobile Intelligent Home Gateway | ✗ | ✗ | ✗ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-87827 | KGUARD DVR Command Execution Vulnerability | KGUARD DVR | ✗ | ✗ | ✗ |
| CVE-2026-105133 | Ahsay AhsayCBS Improper Authentication Vulnerability | Ahsay AhsayCBS | ✓ | ✓ | ✓ |
| CVE-2026-105134 | Ahsay AhsayCBS Command Injection Vulnerability | Ahsay AhsayCBS | ✓ | ✓ | ✓ |
| CVE-2026-107406 | Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability | Citrix NetScaler ADC and NetScaler Gateway | ✗ | ✓ | ✓ |
| CVE-2026-102255 | SonicWall SMA 1000 WorkPlace Pre-Authentication Server-Side Request Forgery Vulnerability | SonicWall SMA 1000 Series | ✗ | ✗ | ✓ |
| CVE-2026-104935 | Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability | Ivanti Connect Secure | ✓ | ✓ | ✓ |
| CVE-2026-96951 | Windows Shell Security Feature Bypass Vulnerability | Windows, Outlook.com | ✓ | ✓ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-92707 | MessagePack-CSharp Denial of Service Vulnerability | Microsoft Visual Studio | ✗ | ✗ | ✓ |
| CVE-2026-108398 | .NET Framework Security Feature Bypass Vulnerability | .NET Framework | ✗ | ✗ | ✓ |
| CVE-2026-76519 | Cisco Secure Email Gateway Relative Path Traversal Vulnerability | Cisco Secure Email Gateway | ✓ | ✓ | ✓ |
| CVE-2026-0322 | Palo Alto Networks PAN-OS Code Injection Vulnerability | Palo Alto Networks PAN-OS | ✓ | ✓ | ✓ |
| CVE-2025-61624 | Fortinet FortiOS CLI Path Traversal Vulnerability | Fortinet FortiOS, FortiPAM, FortiProxy, FortiSwitch Manager | ✗ | ✗ | ✓ |
| CVE-2024-47575 | FortiJump (Fortinet FortiManager Missing Authentication Vulnerability) | Fortinet FortiManager | ✓ | ✓ | ✓ |
| CVE-2026-102764 | BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability | BeyondTrust Remote Support | ✓ | ✓ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-106173 | Fortinet FortiSIEM Path Traversal Vulnerability | Fortinet FortiSIEM | ✗ | ✗ | ✓ |
| CVE-2026-114625 | Arista VeloCloud Orchestrator SQL Injection Vulnerability | Arista VeloCloud Orchestrator (VCO) On-Prem | ✓ | ✓ | ✓ |
| CVE-2026-115560 | PHP Remote Code Execution Vulnerability | PHP (affected versions not disclosed by vendor) | ✗ | ✗ | ✗ |
| CVE-2020-3259 | Cisco ASA and FTD Information Disclosure Vulnerability | Cisco ASA and FTD | ✗ | ✓ | ✓ |
| CVE-2023-20269 | Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability | Cisco Adaptive Security Appliance and Firepower Threat Defense | ✓ | ✓ | ✓ |
| CVE-2023-27532 | Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability | Veeam Backup & Replication, Veeam Cloud Connect | ✗ | ✓ | ✓ |
| CVE-2024-40711 | Veeam Backup and Replication Deserialization Vulnerability | Veeam Backup and Replication | ✗ | ✓ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2024-40766 | SonicWall SonicOS Improper Access Control Vulnerability | SonicWall SonicOS | ✗ | ✓ | ✓ |
| CVE-2026-101767 | Oracle E-Business Suite SQL Injection Vulnerability | Oracle E-Business Suite | ✗ | ✗ | ✓ |
| CVE-2026-109618 | PHP2Shell (PHP Memory Corruption Vulnerability) | PHP Group PHP | ✗ | ✓ | ✓ |
| CVE-2026-109619 | PHP2Shell (PHP Stale Internal Request-State Vulnerability) | PHP Group PHP | ✗ | ✓ | ✓ |
| CVE-2026-111497 | Google Brotli Unchecked Return Value Vulnerability | Node.js, Bun, Google Brotli, Python Brotli, brotlicffi, Microsoft .NET 8, .NET 9, .NET 10, .NET 11 | ✗ | ✓ | ✓ |
| CVE-2026-96652 | Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability | Plex Media Server (Before 1.43.3.10861) | ✗ | ✓ | ✓ |
| CVE-2026-96654 | Plex Media Server Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability | Plex Media Server (Before 1.43.3.10861) | ✗ | ✓ | ✓ |

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-96655 | Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability | Plex Media Server (Before 1.43.3.10861) | ✗ | ✓ | ✓ |
| CVE-2026-96656 | Plex Media Server External Control of File Name or Path Vulnerability | Plex Media Server (Before 1.43.3.10861) | ✗ | ✓ | ✓ |
| CVE-2026-105482 | Node.js DNS Null Byte Truncation Vulnerability | OpenJS Foundation Node.js 26.x (Before 26.12.1), Node.js 24.x (Before 24.22.1), Node.js 22.x (Before 22.23.4) | ✗ | ✗ | ✓ |
| CVE-2026-76418 | Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability | Cisco Secure Firewall ASA Software, Cisco Secure Firewall Threat Defense (FTD) Software | ✓ | ✓ | ✓ |

# Attacks Summary

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| Chopper | Web Shell | CVE-2026-73570 | Zimbra Collaboration Suite servers |  | Exploiting Vulnerability |
| Godzilla | Web Shell | CVE-2026-73570 | Zimbra Collaboration Suite servers |  | Exploiting Vulnerability |
| CoinMiner | Cryptominer | CVE-2026-73570 | Zimbra Collaboration Suite servers |  | Exploiting Vulnerability |
| Looptik | Hacktool | CVE-2026-73570 | Zimbra Collaboration Suite servers |  | Exploiting Vulnerability |
| Zimdown2 | Downloader | CVE-2026-73570 | Zimbra Collaboration Suite servers |  | Exploiting Vulnerability |
| Zimclient2 | Backdoor | CVE-2026-73570 | Zimbra Collaboration Suite servers |  | Exploiting Vulnerability |
| ShelbyLoader | Loader | - | Microsoft Windows | - | Trojanized Visual Studio project |
| ShelbyC2 | Backdoor | - | Microsoft Windows | - | Loaded by ShelbyLoader V2 |
| PsProxy | Post-Exploitation Tool | - | Microsoft Windows | - | Invoked by ShelbyC2 V2 |
| Blackwood | Tunneling loader | - | Microsoft Windows | - | GitHub-hosted ZIP archive |

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| Shai-Hulud | Worm | - | - | - | Malicious code into the tensorlakeai/tensorlake |
| ClingSTUN | Backdoor | CVE-2022-36553<br>CVE-2025-34035<br>CVE-2024-23625<br>CVE-2021-35394<br>CVE-2023-1389<br>CVE-2024-7029<br>CVE-2024-10915<br>CVE-2024-23624<br>CVE-2019-17621<br>CVE-2019-7256<br>CVE-2021-36380<br>CVE-2024-21887<br>CVE-2023-46805<br>CVE-2024-46048<br>CVE-2024-35340<br>CVE-2024-32314<br>CVE-2024-32292<br>CVE-2024-32281<br>CVE-2022-35555<br>CVE-2022-26289<br>CVE-2022-37055<br>CVE-2024-10914<br>CVE-2026-36356<br>CVE-2025-67038<br>CVE-2014-8361<br>CVE-2016-20016<br>CVE-2024-3721<br>CVE-2025-34037<br>CVE-2023-26801<br>CVE-2023-41011<br>CVE-2026-87827 | Linux (IoT devices on ARM, Intel 80386, AMD x86-64, MIPS R3000 and PowerPC) |  | Exploitation of known vulnerabilities |

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| FLATROOF | Backdoor | - | macOS, Windows, Linux | - | Trojanized Terraform |
| ROOFDECK | Backdoor | - | macOS, Windows, Linux | - | FLATROOF drops ROOFDECK as the final stage |
| PEERSTITCH | Backdoor | CVE-2025-61624 CVE-2024-47575 | Fortinet FortiManager, Fortinet FortiGate, Fortinet FortiOS, Fortinet FortiPAM, Fortinet FortiProxy, Fortinet FortiSwitchManager |  | Exploiting Vulnerability |
| Aoki | Infostealer | - | Windows | - | - |
| SAWFLY | Web shell | CVE-2026-102764 | BeyondTrust Remote Support ≤26.2.3 |  | Exploiting vulnerabilities |
| BARECLAW | Proxy tunneler | CVE-2026-102764 | BeyondTrust Remote Support ≤26.2.3 |  | Exploiting vulnerabilities |
| privcollect | Credential stealer | - | LiteLLM (BerriAI) version 1.107.0 | - | Software supply-chain compromise |
| SafePay | Ransomware | CVE-2020-3259, CVE-2023-20269, CVE-2023-27532, CVE-2024-40711, CVE-2024-40766 | Cisco ASA & FTD, Veeam Backup & Replication, SonicWall SonicOS |  | Stolen credentials, edge-device exploits |

| ATTACK NAME | TYPE | CVEs | IMPACTED PRODUCT | PATCH | DELIVERY METHOD |
|---|---|---|---|---|---|
| Sirius Backdoor | Backdoor | - | Windows | - | Phishing |
| XMRig | Cryptominer | CVE-2026-105133, CVE-2026-105134, CVE-2026-96652, CVE-2026-96654, CVE-2026-96655, CVE-2026-96656 | Plex Media Server & Ahsay AhsayCBS |  | Exploiting vulnerabilities |
| myawesome proxy | Proxyware | CVE-2026-96652, CVE-2026-96654, CVE-2026-96655, CVE-2026-96656 | Plex Media Server |  | Exploiting vulnerabilities |

# Adversaries Summary

| ACTOR NAME | MOTIVE | ORIGIN | CVEs | ATTACK | PRODUCT |
|---|---|---|---|---|---|
| UTA0576 | Information Theft | - | CVE-2026-104935 | - | Ivanti Connect Secure |
| TraderTraitor | Financial Gain | North Korea | - | FLATROOF, ROOFDECK | macOS, Windows, Linux |
| CL-STA-0954 | Information Theft | - | CVE-2025-61624, CVE-2024-47575 | PEERSTITCH | Fortinet FortiManager, Fortinet FortiGate, Fortinet FortiOS, Fortinet FortiPAM, Fortinet FortiProxy, Fortinet FortiSwitchManager |
| ARMORY CASTLE | Cyber espionage | China (suspected) | CVE-2026-102764 | SAWFLY, BARECLAW | BeyondTrust Remote Support |
| Lazarus | Information theft and espionage, Sabotage and destruction, Financial crime | North Korea | CVE-2026-109618 CVE-2026-109619 | - | PHP |

# Targeted Products

| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| SYNACOR | Mail & Collaboration Server | Zimbra Collaboration Suite (ZCS) before 10.1.20 |
| citrix | Network Device | NetScaler ADC 14.1-73.41 and earlier, 13.1-64.28 and earlier, NetScaler ADC 14.1-FIPS 14.1-73.41 FIPS and earlier, NetScaler ADC 13.1-FIPS and 13.1-NDcPP 13.1-37.282 and earlier, NetScaler Gateway 14.1-73.41 and earlier, 13.1-64.28 and earlier |
| FORTINET | Security Appliance | FortiMail 8.0.0 through 8.0.1, 7.6.0 through 7.6.6, 7.4.0 through 7.4.8, 7.2.0 through 7.2.9, FortiProxy 7.6.0 through 7.6.4, 7.4.0 through 7.4.11, 7.2 all versions, 7.0 all versions |
| | Operating System | FortiOS 7.6.0 through 7.6.4, 7.4.0 through 7.4.9, 7.2 all versions, 7.0 all versions, 6.4 all versions |
| | Security Software | FortiPAM 1.7.0, 1.6 all versions, 1.5 all versions, 1.4 all versions, 1.3 all versions, 1.2 all versions, 1.1 all versions, 1.0 all versions, FortiSIEM 7.5.0 (before 7.5.1) |
| | Network Management Platform | FortiSwitchManager 7.2.0 through 7.2.7, 7.0.0 through 7.0.6 |

| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| FORTINET | Security Management Platform | FortiManager 7.6.0, 7.4.0 through 7.4.4, 7.2.0 through 7.2.7, 7.0.0 through 7.0.12, 6.4.0 through 6.4.14, 6.2.0 through 6.2.12, FortiManager Cloud 7.4.1 through 7.4.4, 7.2 all versions, 7.0 all versions, 6.4 all versions |
| ATLASSIAN | Source Code Management | Bitbucket Data Center version before 9.4.26/10.2.8/10.5.1 |
| | Collaboration Software | Confluence Data Center version before 9.2.26/10.2.19 |
| | IT Service Management | Jira Service Management Data Center version before 5.12.40/10.3.26/11.3.12 |
| | Project Management Software | Jira Software Data Center version before 9.12.40/10.3.26/11.3.12 |
| | CI/CD Server | Bamboo Data Center versions before 10.2.24/12.1.12 |
| | Identity & Access Management | Crowd Data Center version before 6.3.7/7.0.3/7.1.7/7.2.4 |
| | Code Review Tool | Crucible version before 4.9.15 |
| | Code Repository Browser | Fisheye version before 4.9.15 |
| hytec inter | Network Device | HWL-2511-SS v1.05 and below |
| EnGenius | Network Device | EnShare Cloud Service version 1.4.11 and earlier |
| D-Link | Network Device | DAP-1650 all firmware versions, DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01, GO-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02 |

| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| D-Link | Storage Device (NAS) | DNS-320 up to 20241028, DNS-320LW up to 20241028, DNS-325 up to 20241028, DNS-340L up to 20241028 |
| Realtek | Software Development Kit | Jungle SDK version v2.x up to v3.4.14B, Realtek SDK (no affected version range published) |
| tp-link | Network Device | Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219 |
| AVTECH | Surveillance Device | AVM1203 IP camera firmware FullImg-1023-1007-1011-1009 and prior |
| Nice / LINEAR a Nice brand | Access Control System | Linear eMerge E3-Series (Elite and Essential) firmware 1.00-06 and prior |
| SUNHILLO | Surveillance Data Distribution System | SureLine before 8.7.0.1.1 |
| ivanti | Security Appliance | Connect Secure 9.x, 22.x, 22.8R2.4 and prior, 25.1.1.1 on ISA6000/ISA8000, 25.1.2.2 and prior |
| | Network Access Control | Policy Secure 9.x, 22.x |
| Tenda | Network Device | FH451 v1.0.0.9, FH1206 V1.2.0.8(8155), AC500 V2.0.1.9(1307), W30E v1.0 V1.0.1.25(633), AC7V1.0 v15.03.06.44, W6 V1.0.0.9(4122), M3 1.10 V1.0.0.12(4856) |
| MEIG | Network Device | FORGE_SLT711 devices (firmware MDM9607.LE.1.0-00110-STD.PROD-1) |
| LANTRONIX Innovation Reimagined. | Network Device | EDS5000 2.1.0.0R3 |
| MV POWER SOLUTIONS Electrical Contractors | Surveillance Device | CCTV DVR models, including TV-7104HE 1.8.4 115215B9 and TV7108HE |
| TBK | Surveillance Device | DVR-4104 up to 20240412, DVR-4216 up to 20240412 |

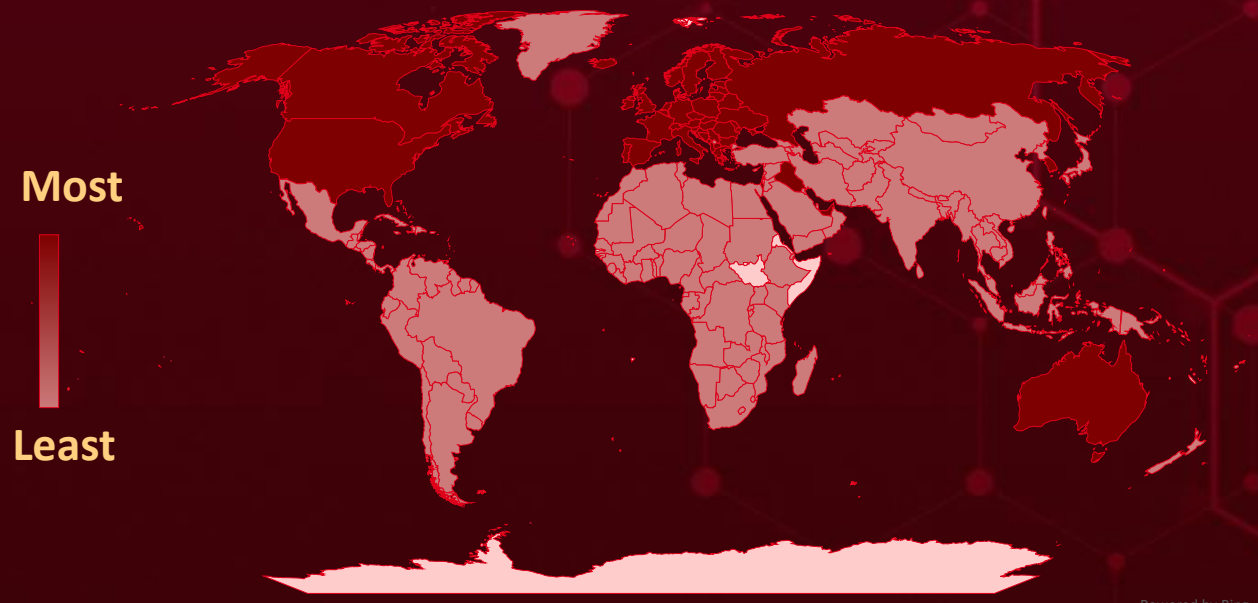
| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| Linksys | Network Device | E4200 before 1.0.06, E3200 before 1.0.05, E3000 before 1.0.06, E2500 v1/v2 before 2.0.00, E2100L v1 1.0.05 and earlier, E2000 all versions, E1550 1.0.03 and earlier, E1500 v1 before 1.0.06, E1200 v1 1.0.04 and earlier, E1000 v1 before 2.1.03, E900 v1 before 1.0.04 |
| LB-LINK | Network Device | BL-AC1900_2.0 v1.0.1, BL-WR9000 v2.4.9, BL-X26 v1.2.5, BL-LTE300 v1.0.8 |
| 中国移动 China Mobile | Network Device | Intelligent Home Gateway v.HG6543C4 |
| KGUARD SECURITY | Surveillance Device | DVR devices running 2016 firmware (firmware released after 2017 binds the service to localhost), including D1004NR, D1008NR, D1016NR, D1104, D1104NR, D1108NR, D1116NR, D1132NR, D2116NR, D97xx, D98xx and D99xx variants |
| Ahsay Backup | Backup Software | AhsayCBS (v10 builds before hotfix 10.3.4.45) |
| SONICWALL | Security Appliance | SMA 1000 Series - 6210, 7210, 8200v (platform-hotfix 12.4.3-03526 and earlier, 12.5.0-02952 and earlier) |
| | Operating System | SonicOS Gen 5 SOHO 5.9.2.14-12o and older, Gen 6 6.5.4.14-109n and older, Gen 7 7.0.1-5035 and older |
| Microsoft | Operating System | Windows 10 - 11 26H2, Windows Server 2012, 2016, 2019, 2022, 2025 |
| | Email Service | Outlook.com |

| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| Microsoft | Developer Tools | Visual Studio 2026 version 18.10 |
| | Software Library | MessagePack 2.5.303 |
| | Development Framework | .NET Framework 3.5 and 4.8.1 on Windows 11 23H2, 24H2, 25H2, 26H2 and Windows Server 2025, .NET 8 (before 8.0.33), .NET 9 (before 9.0.22), .NET 10 (before 10.0.14), .NET 11 (before RC3) |
| CISCO | Security Appliance | Secure Email Gateway (AsyncOS 15.5 before 15.5.5-014, 16.0 all releases, 16.5 before 16.5.0-780, Content Scanner Tools before 25.3.0.5525) |
| | Firewall Software | Secure Firewall ASA Software before 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, 9.24.1.27 / 9.24.10.1, versions before 9.8.4.20, 9.9.2.67, 9.10.1.40, 9.12.3.9, 9.13.1.10, 9.8.x through 9.19.x, Secure Firewall Threat Defense (FTD) Software before 7.0.11, 7.2.13, 7.4.9, 7.6.7, 7.7.14, 10.0.3, 10.1.1, versions before 6.2.3.16, 6.3.0.6, 6.4.0.9, 6.5.0.5, 6.2.3 through 7.4.0 |

| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| paloalto NETWORKS | Operating System | PAN-OS 12.2 (before 12.2.4), 12.1 (before 12.1.4-h12, 12.1.7-h8, 12.1.10-h2), 11.2 (before 11.2.4-h22, 11.2.7-h21, 11.2.10-h15, 11.2.13-h3, 11.2.16), 11.1 (before 11.1.4-h37, 11.1.6-h39, 11.1.7-h11, 11.1.10-h35, 11.1.13-h15, 11.1.16-h3), 10.2 (before 10.2.7-h38, 10.2.10-h41, 10.2.13-h26, 10.2.16-h11, 10.2.18-h12) on PA-Series, VM-Series and Panorama |
| BeyondTrust | Application | Remote Support (26.2.3 and prior) |
| php | Programming Language | PHP 5.4 through 8.5.11 (further affected versions not disclosed by vendor) |
| ARISTA | Network Management Platform | VeloCloud Orchestrator (VCO) On-Prem (5.2.x before 5.2.3.18, 6.1.x before 6.1.3.10, 6.4.x before 6.4.2.12) |
| veeam | Backup Software | Backup & Replication 12.1.2.172 and all earlier version 12 builds, version 11 builds before 11.0.1.1261 P20230227, and all earlier versions, Cloud Connect (Backup & Replication) all versions before 12.0.0.1420 P20230223 and 11.0.1.1261 P20230227 |
| node JS | Runtime Environment | Node.js 22.x (before 22.23.4), 24.x (before 24.22.1), 26.x (before 26.12.1) and End-of-Life versions |
| Bun | Runtime Environment | Bun (before 1.4.4) |
| G | Software Library | Brotli (1.0.3 through 1.2.0), Python Brotli (before 1.2.1) |

| VENDOR | PRODUCT TYPE | PRODUCT WITH VERSION |
|---|---|---|
| hyper | Software Library | brotlicffi (before 1.2.1.0) |
| ORACLE | Application | E-Business Suite (Oracle Application Object Library) 12.2.3 to 12.2.15 |
| PLEX | Application | Plex Media Server (before 1.43.3.10861) |

# Targeted Countries




Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

| Color | Countries |
|---|---|
| | United Kingdom |
| | United States |
| | Australia |
| | United Arab Emirates |
| | Iraq |
| | Belgium |
| | Bosnia and Herzegovina |
| | Bulgaria |
| | Canada |
| | Croatia |
| | Czech Republic |
| | Denmark |
| | Estonia |
| | Finland |
| | France |
| | Germany |
| | Greece |
| | Holy See |
| | Hungary |
| | Iceland |

| Color | Countries |
|---|---|
| | Israel |
| | Italy |
| | Latvia |
| | Liechtenstein |
| | Lithuania |
| | Luxembourg |
| | Malta |
| | Moldova |
| | Monaco |
| | Montenegro |
| | Netherlands |
| | North Macedonia |
| | Norway |
| | Poland |
| | Portugal |
| | Republic of Ireland |
| | Romania |
| | Russia |
| | San Marino |
| | Serbia |

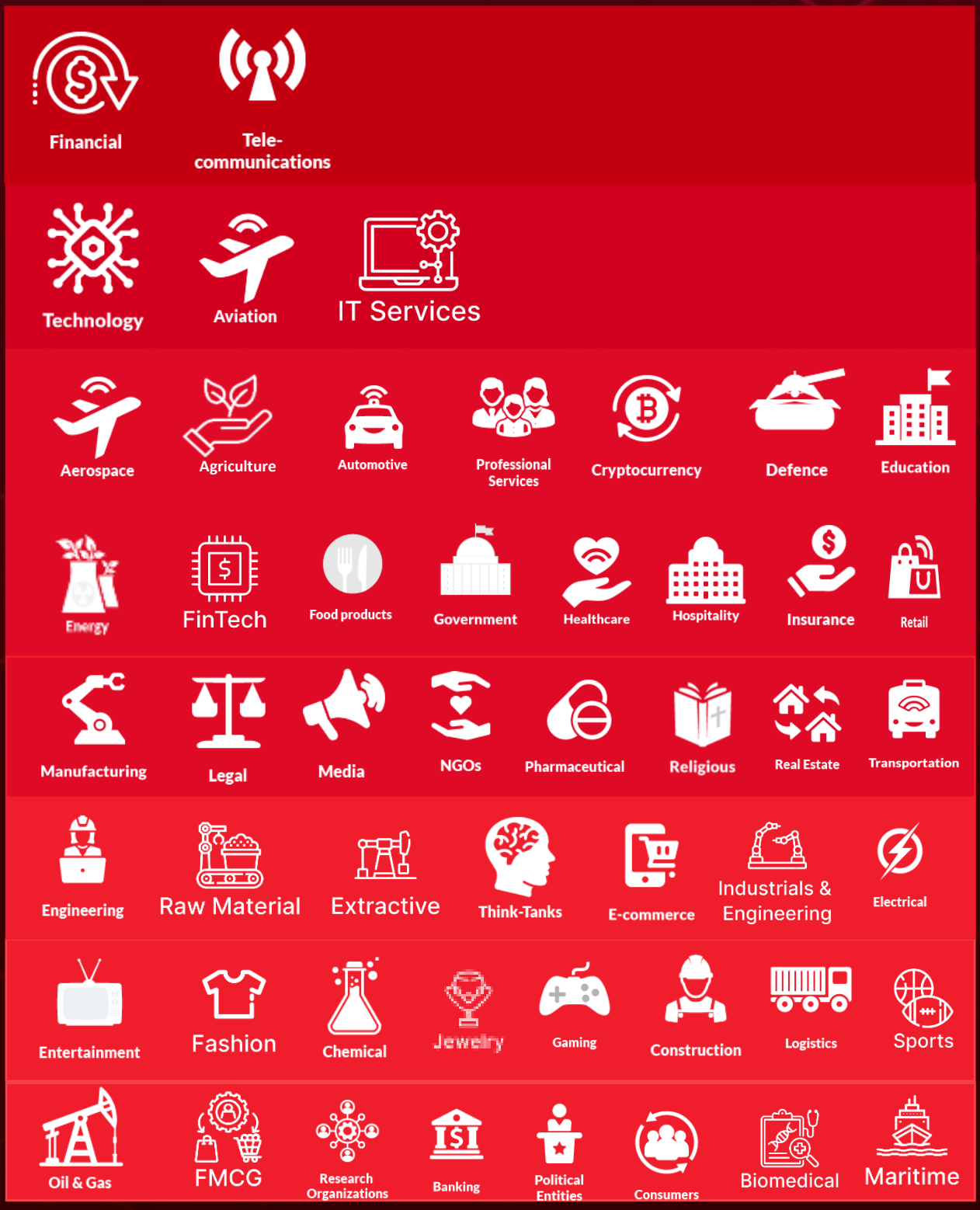
| Color | Countries |
|---|---|
| | South Korea |
| | Spain |
| | Sweden |
| | Switzerland |
| | Ukraine |
| | Austria |
| | Albania |
| | Andorra |
| | Afghanistan |
| | Akrotiri and Dhekelia |
| | Algeria |
| | American Samoa |
| | Angola |
| | Anguilla |
| | Antigua and Barbuda |
| | Argentina |
| | Armenia |
| | Aruba |
| | Slovakia |
| | Slovenia |

| Color | Countries |
|---|---|
| | Azerbaijan |
| | Bahamas |
| | Bahrain |
| | Bangladesh |
| | Barbados |
| | Belize |
| | Benin |
| | Bermuda |
| | Bhutan |
| | Bolivia |
| | Bonaire |
| | Botswana |
| | Brazil |
| | British Virgin Islands |
| | Brunei |
| | Burkina Faso |
| | Burundi |
| | Cambodia |
| | Cameroon |
| | Canada Quebec |

| Color | Countries |
|---|---|
| | Cape Verde |
| | Cayman Islands |
| | Central African Republic |
| | Chad |
| | Chile |
| | China |
| | Colombia |
| | Comoros |
| | Congo-Brazzaville |
| | Costa Rica |
| | Cuba |
| | Curacao |
| | Cyprus |
| | Democratic Republic of Congo |
| | Djibouti |
| | Dominica |
| | Dominican Republic |
| | Ecuador |

# Targeted Industries

Most




Least

# TOP 25 MITRE ATT&CK TTPS

| | | | | |
|---|---|---|---|---|
| **T1190** Exploit Public-Facing Application | **T1059** Command and Scripting Interpreter | **T1071** Application Layer Protocol | **T1105** Ingress Tool Transfer | **T1036** Masqueradin g |
| **T1071.001** Web Protocols | **T1068** Exploitation for Privilege Escalation | **T1588** Obtain Capabilities | **T1552** Unsecured Credentials | **T1005** Data from Local System |
| **T1041** Exfiltration Over C2 Channel | **T1552.001** Credentials In Files | **T1036.005** Match Legitimate Name or Location | **T1059.00 4** Unix Shell | **T1588.006** Vulnerabilities |
| **T1499** Endpoint Denial of Service | **T1027** Obfuscated Files or Information | **T1078** Valid Accounts | **T1505.00 3** Web Shell | **T1496** Resource Hijacking |
| **T1053** Scheduled Task/Job | **T1098** Account Manipulation | **T1140** Deobfuscate/D ecode Files or Information | **T1566** Phishing | **T1505** Server Software Component |

# Top Indicators of Compromise (IOCs)

| Attack Name | TYPE | VALUE |
|---|---|---|
| Chopper | SHA256 | 13d27ecfbb6b3d55bdabcaa3a2ade83ecfaa3df92dbc22be05e6d9e2d18087b6, dc76d856d42242e58eb8d4b70d5378f42f3ddf0ef7872d2279f2d67c22806e26, 5cc6bc95c584d72cc61842f0ee58f38ac4519ec953a2dff3d37e2e8f389f3d54 |
| CoinMiner | SHA256 | aea991f694911e321b0ab97534f2ad0291c392c0a43dabff664c563618bd036d |
| ShelbyLoader | Filename | RuntimeBroker.dll, RuntimeBroker.exe.config, DubaiAirport_Carrers_IT_Test.zip, FlightManager.csproj |
| | SHA256 | 53f35e49eb9b271fd8cbcd3daacb525328dbf159a03dbd1c7adebe0363daa402, 6e7d9b33f1e72ea1ede71373a604ecdb060dab7d42055179c1eede9ecd1fd239, f5b12772db6817f7a765a6fe7565fd3d4f87edc28e42fe3ec0244a372a410fc9 |
| Shai-Hulud | SHA256 | 25a0735d0db7dc40e5d45ce42d9c106067e6a66e184d967cfecfab17c3bcb5ef, b50a00900399ba99fb6ce1fc151519cb99d44320ef2a631f2237e1aea0ad6fec |
| XMRig | SHA256 | 739f7328a5d0912cace9d289d7f2d295117d74580c08a6a02d72c94cba41416e, fcde8af943753f831219c1d1ff82a425ff27b8c8e72dee6e4d64e95912125804, dd752e32f65f4508f86b1cd1d2795e96614b6e76dd4d1d2a686c0b01b6c69b24, a06b4510e3af4b544e617c5ac30267e33df9fed0c5592231b2a1ab3fefb0d8eb, 3c36581fac391feee2b35b385f423d8502f11a80d65e5f5788df8c22ebfc2f43, d8b9b5a48070d6d3774be3ec176b0cd30b40a4da2779f072243d20bd9fc2901f, 23ee60f1bd28f720527167be17861ff7f369ca89e0b0c3cd29ba3849bc3542ff, 155b5c9a6a8a93f249278f7c46a376abe595ac90ddf4771cf2da47805e54529d, 2d3c618b21a7e2f8bcd735da188e44a7609ff3f204832dd0781cd09e4388c9db |

| Attack Name | TYPE | VALUE |
|---|---|---|
| myawesomeproxy | SHA256 | e546b10aee5edc754da4f9b0baace00392257121911f630145078eafad1e6bd9 |
| | Domain | proxystream[.]st |
| FLATROOF | SHA256 | 451b586ec9d3c997b319986a1177829653e8ae641c953c05ede6a38616f2da97 |
| ROOFDECK | SHA256 | e1c71374814e5d907afb913108090b8abf21ae2131c0880f013a3b9108a9d0fc |
| PEERSTITCH | SHA256 | b9fb0b27ddd59b58d3ae53c7227298a3e0de1e6f868b9429ae21533bb9cd1e70 |
| | IPv4 | 23[.]240[.]77[.]233,<br>47[.]18[.]167[.]159 |
| | URL | hxxp[:]//23[.]240[.]77[.]233[:]8085/pM.js,<br>hxxp[:]//47[.]18[.]167[.]159[:]8085/pM.js |
| privcollect | SHA256 | 03ac2a8b752605d1d7710979c17ff18b03dd978203ba23ba97fd8ce3d6f897ea,<br>9dd0a3926f96a37eb86cf1ee2310d9be93139cc4ebef3ef9e2efe9531390be25 |
| SafePay | SHA256 | 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae,<br>6c1d36df94ebe367823e73ba33cfb4f40756a5e8ee1e30e8f0ae55d47e220a6a,<br>e79608cf1d6b51324c14bef8883054c1238ed5f080222cc464810e6e14adc346,<br>327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917,<br>a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526 |
| | SHA1 | 07353237350c35d6dc2c8f143b649cd07c71f62b,<br>b498a2683640c983bb069fa2ea9e67cef4a3797d,<br>BBFED53E3BB1F306F4DA97D995CF4AE5B73AD081 |
| | IPv4 | 77[.]37[.]49[.]40,<br>167[.]235[.]225[.]149,<br>5[.]255[.]11[.]134,<br>37[.]10[.]71[.]188,<br>88[.]119[.]167[.]239 |
| | Email | ColinSolomon[@]protonmail[.]com |
| | Filename | locker.dll |

| Attack Name | TYPE | VALUE |
|---|---|---|
| SafePay | Filename | soc.dll,<br>readme_safepay.txt,<br>Socks_werfault.exe,<br>DYRasWtb.exe |
| | Hostname | WIN-SBOE3CPNALE,<br>WIN-3IUUOFVTQAR,<br>WIN-DK18BI83M0S,<br>WIN-I1HRRJHCEIV |

# Vulnerabilities Exploited

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-73570 |  | Synacor Zimbra Collaboration Suite (ZCS) Before 10.1.20 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:synacor:zimbra_collaboration_suite:*:*:*:*:*:*:*:* | Chopper, Godzilla Web Shell, CoinMiner, Looptik, Zimdown2, Zimclient2 |
| Zimbra Collaboration Suite (ZCS) OS Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINKS |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1505: Server Software Component, T1505.003: Web Shell | https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-88779 |  | Citrix NetScaler ADC and NetScaler Gateway 14.1 (Before 14.1-73.41), Citrix NetScaler ADC and NetScaler Gateway 13.1 (Before 13.1-64.28), Citrix NetScaler ADC 14.1-FIPS (Before 14.1-73.41 FIPS), Citrix NetScaler ADC 13.1-FIPS and 13.1-NDcPP (Before 13.1-37.282) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:*:*, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*:*, cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:*, cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:* | - |
| Citrix NetScaler Improper Restriction of Operations within the Bounds of a Memory Buffer Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-119 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer, T1505: Server Software Component | https://support.citrix.com/external/article/CTX697174/citrix-netscaler-adc-and-citrix-netscale.html |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-104286 |  | Fortinet FortiMail 8.0.0 through 8.0.1, 7.6.0 through 7.6.6, 7.4.0 through 7.4.8, 7.2.0 through 7.2.9 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*:*:* | - |
| Fortinet FortiMail Path Traversal Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-22, CWE-158 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://fortiguard.fortinet.com/psirt/FG-IR-26-175 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-21589 | ✗ | Atlassian Bitbucket Data Center Version before 9.4.26,10.2.8, 10.5.1, Confluence Data Center Version before 9.2.26, 10.2.19, Jira Service Management Data Center Version before 5.12.40,10.3.26, 11.3.12, Jira Software Data Center Version before 9.12.40, 10.3.26,11.3.12, Bamboo Data Center Versions before 10.2.24,12.1.12, Crowd Data Center Version before 6.3.7, 7.0.3,7.1.7,7.2.4, Crucible Version before 4.9.15 and Fisheye Version before 4.9.15 | - |
| | ZERO-DAY | | |
| | ✗ | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:atlassian:bitbucket:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:confluence:*:*:*:*:*:data _center:*:*:*, cpe:2.3:a:atlassian:jira_service_management:*:*:*:*:*:data_center:*:*:*, cpe:2.3:a:atlassian:jira_software:*:*:*:*:*:da ta_center:*:*:*, cpe:2.3:a:atlassian:bamboo:*:*:*:*:*:data_ce nter:*:*:*, cpe:2.3:a:atlassian:crowd:*:*:*:*:*:data_cen ter:*:*:*, cpe:2.3:a:atlassian:crucible:*:*:*:*:*:*:*:*:*:*:*, cpe:2.3:a:atlassian:fisheye:*:*:*:*:*:*:*:*:* | - |
| Atlassian Multiple Products Arbitrary File Access Vulnerability | ✗ | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-552 | T1190: Exploit Public-Facing Application, T1552: Unsecured Credentials | https://confluence.atlassian.com/security/cve-2026-21589-arbitrary-file-access-vulnerability-impacts-multiple-products-1870495748.html |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2022-36553</td><td>✗</td><td rowspan="2">Hytec Inter HWL-2511-SS v1.05 and below</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:hytec:hwl-2511-ss_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">ClingSTUN Backdoor</td></tr>
<tr><td rowspan="3">Hytec Inter HWL-2511-SS Command Injection Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer</td><td>-</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2025-34035 |  | EnGenius EnShare Cloud Service version 1.4.11 and earlier. | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:h:engeniustech:esr300:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| EnGenius EnShare Cloud Service OS Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-23625 | ✗ | D-Link DAP-1650 devices | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dlink:dap-1650_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| D-Link UPnP SUBSCRIBE Code Injection Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2021-35394 |  | Realtek Jungle SDK version v2.x up to v3.4.14B | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:realtek:rtl819x_jungle_software_development_kit:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Realtek Jungle SDK Remote Code Execution Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell | https://www.realtek.com/images/safe-report/Realtek_APRouter_SDK_Advisory-CVE-2021-35392_35395.pdf |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2023-1389 |  | TP-Link Archer AX21 (AX1800) firmware versions before 1.1.4 Build 20230219 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:tp-link:archer_ax21_firmware:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| TP-Link Archer AX-21 Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1584: Compromise Infrastructure, T1584.008: Network Devices | https://www.tp-link.com/us/support/download/archerax21/v3/#Firmware |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2024-7029</td><td></td><td rowspan="2">AVTECH AVM1203</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:avtech:avm1203_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">ClingSTUN Backdoor</td></tr>
<tr><td rowspan="3">AVTECH AVM1203 Command Injection Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1584: Compromise Infrastructure, T1584.005: Botnet</td><td>-</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-10915 |  | D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dlink:dns-320_firmware:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| D-Link Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-707, CWE-74, CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-23624 | ✗ | D-Link DAP-1650 devices | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dlink:dap-1650_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| D-Link DAP-1650 Command Injection Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2019-17621 |  ZERO-DAY | D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01 | - |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dlink:dir-859_firmware:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| D-Link DIR-859 Router Command Execution Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell | https://www.dlink.com/en/security-bulletin |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2019-7256 |  | Linear eMerge E3-Series devices | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:nortekcontrol:linear_emerge_essential_firmware:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Nice Linear eMerge E3-Series OS Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | https://linear-solutions.com/software-downloads/ |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2021-36380 |  | Sunhillo SureLine before 8.7.0.1.1 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:sunhillo:sureline:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Sunhillo SureLine OS Command Injection Vulnerablity |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | https://www.sunhillo.com/product/sureline/ |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-21887 |  ZERO-DAY | Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure (9.x, 22.x) | - |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:ivanti:policy_secure:-:*:*:*:*:*:*:*, cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Ivanti Connect Secure and Policy Secure Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1505: Server Software Component, T1505.003: Web Shell | https://hub.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2023-46805</td><td></td><td rowspan="2">Ivanti ICS 9.x, 22.x and Ivanti Policy Secure</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ivanti:policy_secure:-:*:*:*:*:*:*:*, cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*</td><td rowspan="2">ClingSTUN Backdoor</td></tr>
<tr><td rowspan="3">Ivanti Connect Secure and Policy Secure Authentication Bypass Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-287</td><td>T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell</td><td>https://hub.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-46048 |  | Tenda FH451 v1.0.0.9 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:tenda:fh451_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Tenda exeCommand Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-35340 |  | Tenda FH1206 V1.2.0.8(8155) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:tenda:fh1206_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Tenda exeCommand Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-32314 |  | Tenda AC500 V2.0.1.9(1307) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:tenda:ac500_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Tenda AC500 formexeCommand Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1078: Valid Accounts, T1078.001: Default Accounts | - |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2024-32292</td><td></td><td rowspan="2">Tenda W30E v1.0 V1.0.1.25(633)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:tenda:w30e_firmware:-:*:*:*:*:*:*:*</td><td rowspan="2">ClingSTUN Backdoor</td></tr>
<tr><td rowspan="3">Tenda exeCommand Command Injection Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer</td><td>-</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-32281 | ✗ | Tenda AC7V1.0 v15.03.06.44 | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:tenda:ac7_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Tenda exeCommand Command Injection Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-77 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2022-35555 |  | Tenda W6 V1.0.0.9(4122) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:tenda:w6_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Tenda W6 exeCommand Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2022-26289 | ✗ | Tenda M3 1.10 V1.0.0.12(4856) | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:tenda:m3_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Tenda exeCommand Command Injection Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2022-37055 |  | D-Link Go-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dlink:go-rt-ac750_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| D-Link Routers Buffer Overflow Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-120 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation | EOL |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-10914 |  | D-Link DNS-320, DNS-320LW, DNS-325 and DNS-340L up to 20241028 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dlink:dns-320_firmware:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| D-Link NAS Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-707, CWE-74, CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | EOL |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-36356 |  | MeiG Smart FORGE_SLT711 devices (firmware MDM9607.LE.1.0-00110-STD.PROD-1) | - |
| | ZERO-DAY | | |
| |  | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | - | ClingSTUN Backdoor |
| MeiG Smart FORGE_SLT711 GoAhead Command Injection Vulnerability |  | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-306, CWE-78 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer | - |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-67038</td><td></td><td rowspan="2">Lantronix EDS5000 2.1.0.0R3</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:lantronix:eds5008_firmware:*:*:*:*:*:*:*:*</td><td rowspan="2">ClingSTUN Backdoor</td></tr>
<tr><td rowspan="3">Lantronix EDS5000 Code Injection Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-78</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1105: Ingress Tool Transfer</td><td>https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/pages/2538438657</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2014-8361 |  | Realtek SDK | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:dlink:dir-905l_firmware:*:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| Realtek SDK Improper Input Validation Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | - | T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer | https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10055 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2016-20016 | ✗ | MVPower CCTV DVR models, including TV-7104HE 1.8.4 115215B9 and TV7108HE | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:mvpower:tv-7104he_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| MVPower Remote Command Execution Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1210: Exploitation of Remote Services, T1505: Server Software Component, T1505.003: Web Shell, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2024-3721 | ✗ | TBK DVR-4104 and DVR-4216 up to 20240412 | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | - | ClingSTUN Backdoor |
| TBK DVR OS Command Injection Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer | EOL |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2025-34037 |  | Linksys E-Series Routers | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | - | ClingSTUN Backdoor |
| Linksys E-Series Routers OS Command Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-78 | T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2023-26801 |  | LB-LINK BL-AC1900_2.0 v1.0.1, LB-LINK BL-WR9000 v2.4.9, LB-LINK BL-X26 v1.2.5, and LB-LINK BL-LTE300 v1.0.8 | - |
| | ZERO-DAY | | |
| |  | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:o:lb-link:bl-lte300_firmware:-:*:*:*:*:*:*:* | ClingSTUN Backdoor |
| lb-link bl-lte300_firmware Command Injection Vulnerability |  | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-77 | T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer | - |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2023-41011</td><td>✗</td><td rowspan="2">China Mobile Communications China Mobile Intelligent Home Gateway v.HG6543C4</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:chinamobile:intelligent_home_gateway_firmware:-:*:*:*:*:*:*:*</td><td rowspan="2">ClingSTUN Backdoor</td></tr>
<tr><td rowspan="3">China Mobile Intelligent Home Gateway Command Execution Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77</td><td>T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer</td><td>-</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-87827 | ✗ | KGUARD DVR | - |
| | ZERO-DAY | | |
| | ✗ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | - | ClingSTUN Backdoor |
| KGUARD DVR Command Execution Vulnerability | ✗ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-1188 | T1210: Exploitation of Remote Services, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1570: Lateral Tool Transfer | - |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-105133 |  | Ahsay AhsayCBS (v10 builds before hotfix 10.3.4.45) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:ahsay:ahsaycbs:*:*:*:*:*:*:*:* | XMRig |
| Ahsay AhsayCBS Improper Authentication Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-287 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://idp3.ahsay.com/idp/Authn/RemoteUser |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-105134</td><td></td><td rowspan="2">Ahsay AhsayCBS (v10 builds before hotfix 10.3.4.45)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ahsay:ahsaycbs:*:*:*:*:*:*:*:*</td><td rowspan="2">XMRig</td></tr>
<tr><td rowspan="3">Ahsay AhsayCBS Command Injection Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-77, CWE-78</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://idp3.ahsay.com/idp/Authn/RemoteUser</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-107406</td><td></td><td rowspan="2">Citrix NetScaler ADC and NetScaler Gateway (14.1-73.41 and earlier, 13.1- 64.28 and earlier), Citrix NetScaler ADC 14.1-FIPS (14.1-73.41 FIPS and earlier), Citrix NetScaler ADC 13.1-FIPS and 13.1- NDcPP (13.1-37.282 and earlier)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:*:*, cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-119</td><td>T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service</td><td>https://support.citrix.com/external/article/CTX697191/citrix-netscaler-adc-and-citrix-netscale.html</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-102255 |  | SonicWall SMA 1000 Series - 6210, 7210, 8200v (platform-hotfix 12.4.3-03526 and earlier; 12.5.0-02952 and earlier) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:sonicwall:sma_1000:*:*:*:*:*:*:*:* | - |
| SonicWall SMA 1000 WorkPlace Pre-Authentication Server-Side Request Forgery Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-918, CWE-441 | T1190: Exploit Public-Facing Application | https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017 |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-104935</td><td></td><td rowspan="2">Ivanti Connect Secure (22.8R2.4 and prior; 25.1.1.1 on ISA6000/ISA8000; 25.1.2.2 and prior)</td><td rowspan="2">UTA0576</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:ivanti:connect_secure:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Ivanti Connect Secure Authentication Bypass by Spoofing Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-290</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://hub.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-CVE-2026-104935?language=en_US</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-96951</td><td></td><td rowspan="2">Windows 10 - 11 26H2, Windows Server 2012, 2016, 2019, 2025, 2022, Outlook.com</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:microsoft:outlook_web:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td>Windows Shell Security Feature Bypass Vulnerability</td><td></td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-77, CWE-78</td><td>T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-96951</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-92707 |  | Microsoft Visual Studio 2026 version 18.10, MessagePack 2.5.303 | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:messagepack:messagepack:*:*:*:*:*:*:*:* | - |
| MessagePack-CSharp Denial of Service Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-1325 | T1499 : Endpoint Denial of Service | https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-92707 |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-108398</td><td></td><td rowspan="2">.NET Framework</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:microsoft:.net_framework:*:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">.NET Framework Security Feature Bypass Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-426</td><td>T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-108398</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-76519 | ✗ | Cisco Secure Email Gateway (AsyncOS 15.5 before 15.5.5-014, 16.0 all releases, 16.5 before 16.5.0- 780; Content Scanner Tools before 25.3.0.5525) | - |
| | ZERO-DAY | | |
| | ✓ | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:cisco:secure_email_gateway:*:*:*:*:*:*:*:* | - |
| Cisco Secure Email Gateway Relative Path Traversal Vulnerability | ✓ | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-23 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxp |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-0322 | ✗ | Palo Alto Networks PAN-OS 12.2 (Before 12.2.4), 12.1 (Before 12.1.4-h12, 12.1.7-h8, 12.1.10-h2), 11.2 (Before 11.2.4-h22, 11.2.7-h21, 11.2.10- h15, 11.2.13-h3, 11.2.16), 11.1 (Before 11.1.4-h37, 11.1.6- h39, 11.1.7-h11, 11.1.10-h35, 11.1.13- h15, 11.1.16-h3), 10.2 (Before 10.2.7-h38, 10.2.10-h41, 10.2.13- h26, 10.2.16-h11, 10.2.18-h12) on PA- Series, VM-Series and Panorama | - |
| | ZERO-DAY | | |
| | ✓ | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:o:palo_alto_networks:pan-os:*:*:*:*:*:*:*:* | - |
| Palo Alto Networks PAN-OS Code Injection Vulnerability | ✓ | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-94 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation | https://security.paloaltonetworks.com/CVE-2026-0322 |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-61624</td><td></td><td rowspan="2">Fortinet FortiOS, FortiPAM, FortiProxy, FortiSwitch Manager</td><td rowspan="2">CL-STA-0954</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*,<br>cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*,<br>cpe:2.3:o:fortinet:fortipam:*:*:*:*:*:*:*:*:*,<br>cpe:2.3:a:fortinet:fortiswitchmanager:*:*:*:*:*:*:*:*:*</td><td rowspan="2">PEERSTITCH</td></tr>
<tr><td>Fortinet FortiOS CLI Path Traversal Vulnerability</td><td></td></tr>
<tr><td></td><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-22</td><td>T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-26-122</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-102764 |  | BeyondTrust Remote Support (26.2.3 and prior) | ARMORY CASTLE (aka UNC5221, WARP PANDA) |
| | **ZERO-DAY** | | |
| |  | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:beyondtrust, :remote_support:*:*:, *:*:*:*:*:*:* | SAWFLY, BARECLAW |
| BeyondTrust Remote Support Authentication Bypass by Spoofing Vulnerability |  | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-290 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://www.beyondtrust.com/trust-center/security-advisories/bt26-05 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-106173 |  | Fortinet FortiSIEM (7.5.0, before 7.5.1) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:fortinet:fortisiem:*:*:*:*:*:*:*:*:* | - |
| Fortinet FortiSIEM Path Traversal Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-22 | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | https://fortiguard.fortinet.com/psirt/FG-IR-26-180 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-114625 |  | Arista VeloCloud Orchestrator (VCO) On-Prem (5.2.x before 5.2.3.18, 6.1.x before 6.1.3.10, 6.4.x before 6.4.2.12) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:arista:velocloud_orchestrator:*:*:*:*:*:*:*:* | - |
| Arista VeloCloud Orchestrator SQL Injection Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | CWE-89 | T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation | https://www.arista.com/en/support/advisories-notices/security-advisory/24838-security-advisory-0199 |

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-115560 |  | PHP (affected versions not disclosed by vendor) | - |
| | ZERO-DAY | | |
| |  | AFFECTED CPE | ASSOCIATED ATTACKS/RANSOMWARE |
| NAME | CISA KEV | cpe:2.3:a:php:php:*:*:*:*:*:*:*:* | - |
| PHP Remote Code Execution Vulnerability |  | | |
| | CWE ID | ASSOCIATED TTPs | PATCH LINK |
| | - | T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter | - |

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2020-3259</td><td></td><td rowspan="2">Cisco ASA and FTD</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:*,<br>cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:*</td><td rowspan="2">SafePay Ransomware</td></tr>
<tr><td rowspan="3">Cisco ASA and FTD Information Disclosure Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-200</td><td>T1190: Exploit Public-Facing Application, T1212: Exploitation for Credential Access</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2023-20269</td><td></td><td rowspan="2">Cisco Adaptive Security Appliance and Firepower Threat Defense</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:*,<br>cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:*</td><td rowspan="2">SafePay Ransomware</td></tr>
<tr><td rowspan="3">Cisco Adaptive Security Appliance and Firepower Threat Defense Unauthorized Access Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-288</td><td>T1190: Exploit Public-Facing Application, T1110: Brute Force, T1133: External Remote Services</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2023-27532</td><td></td><td rowspan="2">Veeam Backup & Replication, Veeam Cloud Connect</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*</td><td rowspan="2">SafePay Ransomware</td></tr>
<tr><td rowspan="3">Veeam Backup & Replication Cloud Connect Missing Authentication for Critical Function Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-306</td><td>T1190: Exploit Public-Facing Application, T1212: Exploitation for Credential Access</td><td>https://www.veeam.com/kb4424</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2024-40711</td><td></td><td rowspan="2">Veeam Backup and Replication</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:veeam:veeam_backup_\&_replication:*:*:*:*:*:*:*:*</td><td rowspan="2">SafePay Ransomware</td></tr>
<tr><td rowspan="3">Veeam Backup and Replication Deserialization Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-502</td><td>T1190: Exploit Public-Facing Application, T1136.001: Create Account: Local Account</td><td>https://www.veeam.com/kb4649</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2024-40766</td><td></td><td rowspan="2">SonicWall SonicOS</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:o:sonicwall:sonicos:*:*:*:*:*:*:*:*</td><td rowspan="2">SafePay Ransomware</td></tr>
<tr><td rowspan="3">SonicWall SonicOS Improper Access Control Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-284</td><td>T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1078: Valid Accounts</td><td>https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-101767</td><td></td><td rowspan="2">Oracle E-Business Suite (Oracle Application Object Library) 12.2.3 to 12.2.15</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td></td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:oracle:appl, ication_object_librar, y:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Oracle E-Business Suite SQL Injection Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-287, CWE-306</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter</td><td>https://www.oracle.com/security-alerts/cpuoct2026.html</td></tr>
</table>

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-105482</td><td>✗</td><td rowspan="2">OpenJS Foundation Node.js 26.x (Before 26.12.1), Node.js 24.x (Before 24.22.1), Node.js 22.x (Before 22.23.4)</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✗</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:nodejs:node.js:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Node.js DNS Null Byte Truncation Vulnerability</td><td>✗</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-284</td><td>T1190: Exploit Public-Facing Application, T1071: Application Layer Protocol</td><td>https://nodejs.org/en/blog/release/v22.23.4/, https://nodejs.org/en/blog/release/v24.22.1/, https://nodejs.org/en/blog/release/v26.12.1/</td></tr>
</table>

| CVE ID | CELEBRITY VULNERABILITY | AFFECTED PRODUCT | ASSOCIATED ACTORS |
|---|---|---|---|
| CVE-2026-76418 |  | Cisco Secure Firewall ASA Software (Before 9.16.4.104, 9.18.4.96, 9.20.4.50, 9.22.3.200, 9.23.1.48, 9.24.1.27 / 9.24.10.1); Cisco Secure Firewall Threat Defense (FTD) Software (Before 7.0.11, 7.2.13, 7.4.9, 7.6.7, 7.7.14, 10.0.3, 10.1.1) | - |
| | ZERO-DAY | | |
| |  | **AFFECTED CPE** | **ASSOCIATED ATTACKS/RANSOMWARE** |
| **NAME** | **CISA KEV** | cpe:2.3:a:cisco:adaptive_security_appliance_software:*:*:*:*:*:*:*:*:*, cpe:2.3:a:cisco:firepower_threat_defense:*:*:*:*:*:*:*:*:* | - |
| Cisco Secure Firewall ASA Software and Cisco Secure FTD Software Unchecked Return Value to NULL Pointer Dereference Vulnerability |  | | |
| | **CWE ID** | **ASSOCIATED TTPs** | **PATCH LINK** |
| | CWE-690 | T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75 |

# Attacks Executed

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Chopper | Chopper is a JSP web shell planted on Zimbra mail servers after exploitation of CVE-2026-73570. Attackers use the command injection flaw to make a web directory writable, decode an encoded payload into a JSP file there, and then restore the original permissions. The web shell gives them ongoing access to the server over HTTP. Copies were spread to other mailbox servers in the same cluster, so deleting one copy does not remove the attacker. | Exploiting Vulnerability | CVE-2026-73570 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Web Shell | | Remote Access, Command Execution, Persistent Access, Lateral Spread | Zimbra Collaboration Suite servers |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| - | | | https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>Godzilla</td><td rowspan="6">Godzilla is a JSP web shell found on Zimbra mail servers compromised through CVE-2026-73570. Attackers use the command injection flaw to make a web directory writable, write the decoded web shell into it, and then restore the original permissions so the change is harder to spot. Once it’s planted, they can come back to the server over HTTP whenever they like. Copies were spread to other mailbox servers in the same cluster, so removing one copy doesn’t end their access.</td><td>Exploiting Vulnerability</td><td>CVE-2026-73570</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Web Shell</td><td rowspan="4">Remote Access, Command Execution, Persistent Access</td><td>Zimbra Collaboration Suite servers</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINKS</td></tr>
<tr><td>-</td><td>https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>CoinMiner</td><td rowspan="6">CoinMiner is a cryptocurrency miner deployed on Zimbra mail servers compromised through CVE-2026-73570. It is pulled from an attacker-controlled server and saved as a hidden file named to look like a legitimate kernel worker process. Cron entries relaunch it every minute and at every reboot. It kills competing miners and redirects their mining pools by editing the system’s hosts file, so the attacker gets the server’s full computing power.</td><td>Exploiting Vulnerability</td><td>CVE-2026-73570</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Cryptominer</td><td rowspan="3">Resource Hijacking, Persistent Execution, Configuration Tampering</td><td>Zimbra Collaboration Suite servers</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINKS</td></tr>
<tr><td>-</td><td>https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Looptik | Looptik is a public privilege escalation toolkit hosted on GitHub that attackers turned into a malicious payload on Zimbra mail servers compromised through CVE-2026-73570. It was planted in memory-backed temporary storage under a hidden name, ready to raise the attacker's access from the limited Zimbra service account toward full system control. | Exploiting Vulnerability | CVE-2026-73570 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Hacktool | | Privilege Escalation, System Compromise | Zimbra Collaboration Suite servers |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| - | | | https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Zimdown2 | Zimdown2 is a Go-based installer used on Zimbra mail servers compromised through CVE-2026-73570. It downloads the Zimclient2 remote access agent, checks the file's hash before installing it, and picks a writable install location and a file name generated at runtime to suit each host. It reports installation progress to the attackers over a separate WebSocket channel, kept apart from the server hosting the payloads. | Exploiting Vulnerability | CVE-2026-73570 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Downloader | | Payload Installation, Remote Access, Data Exposure | Zimbra Collaboration Suite servers |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| - | | | https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Zimclient2 | Zimclient2 is a remote access agent planted on Zimbra mail servers compromised through CVE-2026-73570. It gives attackers an interactive shell, lets them move files to and from the server, and acts as a SOCKS5 proxy so they can reach deeper into the victim's network through the compromised server. It talks to its command servers over WebSocket, TLS or raw TCP and switches between them if one is blocked. To survive reboots and cleanup, it sets up systemd services, OpenRC scripts, cron jobs, shell startup files, SSH keys and new local accounts. | Exploiting Vulnerability | CVE-2026-73570 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Backdoor | | Remote Control, Persistent Access, Data Exfiltration, Network Pivoting | Zimbra Collaboration Suite servers |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| - | | | https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.20#Security_Fixes, https://wiki.zimbra.com/wiki/Zimbra_Releases/10.1.0/patch_installation |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| ShelbyLoader | A C# loader (RuntimeBroker.dll) sideloaded through AppDomainManager hijacking. It checks for sandboxes, sets Run-key persistence, fingerprints the host and beacons to GitHub C2, falling back to dead drops hidden in issue comments, before decrypting ShelbyC2 V2. | Trojanized Visual Studio project | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Loader | | Persistence, payload delivery | Microsoft Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| ShelbyC2 | The primary .NET backdoor (RuntimeBrokerApi.dll), stored AES-encrypted and decrypted in memory with a key derived from GitHub-hosted content. It runs operator commands through PsProxy and stages Blackwood for tunneling. | Loaded by ShelbyLoader V2 | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Backdoor | | Remote command execution | Microsoft Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| PsProxy | An in-memory module that executes PowerShell and has no network or persistence of its own. It hooks System.Management.Automation.dll and runs scripts in a hidden runspace without launching PowerShell.exe. | Invoked by ShelbyC2 V2 | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Post-Exploitation Tool | | Stealthy script execution | Microsoft Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Blackwood | A .NET loader pulled as Client.zip from GitHub and sideloaded into a signed vshost32.exe. It decrypts and reflectively loads an embedded Chisel DLL, then opens a reverse SOCKS proxy for covert pivoting. | GitHub-hosted ZIP archive | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Tunneling loader | | Covert network pivoting | Microsoft Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>Shai-Hulud</td><td rowspan="6">Shai-hulud is a supply-chain worm hidden in compromised packages that executes automatically on install via a bundled bundle.js. Once running, it leverages legitimate tooling to hunt for secrets, scans the host and developer environments for cloud and CI tokens, and validates any credentials it finds, so stolen tokens are immediately usable. The worm then abuses those credentials to propagate, injecting unauthorized GitHub Actions workflows into repositories and moving laterally across accounts, while exfiltrating harvested secrets to a hardcoded webhook. It targets packages from multiple maintainers and automates both secret discovery and repository-level persistence.</td><td>Malicious code into the tensorlakeai/tensorlake</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Worm</td><td rowspan="3">System Compromise, exfiltrates data</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>ClingSTUN</td><td rowspan="6">ClingSTUN is a Linux backdoor that takes over Internet-facing IoT devices. A shell downloader installs it, and it then persists through system startup scripts and hides its process. It kills competing malware and disables the device watchdog so the device doesn’t reboot. It uses public STUN servers to find the device’s external IP address and port mappings, then turns the device into a back-connect proxy that can also run remote commands. It spreads to other devices using built-in exploits.</td><td>Exploitation of known vulnerabilities</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Backdoor</td><td rowspan="3">Remote Control, Command Execution, Proxy Abuse, Persistent Infection, Process Concealment</td><td>-</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>-</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| FLATROOF | FLATROOF is a Rust-based cross-platform backdoor for Windows, macOS, and Linux. It uses platform-specific persistence and multiple backup C2 channels. It can use the Telegram Bot API, GitHub API polling, or an attacker-controlled HTTP webhook for C2. It runs Python scripts that steal sensitive data, and then drops the ROOFDECK backdoor to give the attacker full remote control. | Trojanized Terraform | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Backdoor | | Credential Theft, Cookie Theft, Wallet Theft, Data Exfiltration | macOS, Windows, Linux |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| TraderTraitor | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>ROOFDECK</td><td rowspan="6">ROOFDECK is a backdoor found in Windows and macOS variants, and the two versions have nearly identical functionality. Its key feature is a layered C2 discovery process. It first uses a locally stored address, then pulls a signed and encrypted address from Pastebin, and finally falls back to Nostr profile metadata to find the current Pastebin dead drop. It checks an RSA signature before accepting the server address, so only the operator can redirect infected systems. After it finds the server, it communicates over HTTP and WebSocket.</td><td>FLATROOF drops ROOFDECK as the final stage</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Backdoor</td><td rowspan="3">System Discovery, Command Execution, Reverse Shell</td><td>macOS, Windows, Linux</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>TraderTraitor</td><td>-</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| PEERSTITCH | PEERSTITCH is a small Linux ARM64 program (written in C) that attacks FortiOS devices. It runs once and injects malicious code into the memory of two core FortiOS processes, so it leaves no files on disk. It also sets up a hidden communication channel between those processes inside memory. This lets attackers stay on the device for a long time without being noticed by normal monitoring tools. | Exploiting Vulnerability | CVE-2025-61624<br>CVE-2024-47575 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Backdoor | | Stealthy persistent firewall compromise. | Fortinet FortiManager, Fortinet FortiGate, Fortinet FortiOS, Fortinet FortiPAM, Fortinet FortiProxy, Fortinet FortiSwitchManager |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| CL-STA-0954 | | | https://fortiguard.fortinet.com/psirt/FG-IR-26-122, https://www.fortiguard.com/psirt/FG-IR-24-423 |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Aoki | Aoki (aka Aokigahara) is an infostealer, first seen in early 2026, that is still being actively developed. Recent versions add the theft of credential, token and session files from AI coding assistants such as Claude, OpenAI Codex, Cursor, Codeium, Gemini, GitHub Copilot, JetBrains AI Assistant and Kiro, along with AWS credentials. It also steals data from dozens of browsers, cryptocurrency wallets and extensions, password managers, Discord and Telegram clients, gaming platforms, email clients, and VPN and FTP clients. It records which security products are installed. It has no backdoor command list and sends everything it collects to its C&C server through a /gate endpoint. | - | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Infostealer | | Credential Theft, Token Theft, Session Hijacking, Cryptocurrency Theft, Financial Fraud | Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| SAWFLY | A lightweight PHP web shell deployed after successful compromise of BeyondTrust Remote Support appliances, giving interactive remote access and encrypted two-way command-and-control. The actor uses it as the conduit to escalate privileges, take full administrative control of the appliance, and keep persistence that survives reboots. | Exploiting vulnerabilities | CVE-2026-102764 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Web shell | | Remote access, persistence | BeyondTrust Remote Support ≤26.2.3 |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| ARMORY CASTLE | | | https://www.beyondtrust.com/trust-center/security-advisories/bt26-05 |

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| BARECLAW | A custom C-based SOCKS5 proxy tunneler that relays TCP connections between a remote client and destinations through the compromised appliance. The actor modifies the appliance's HAProxy configuration so the tunneler can be reached directly from the internet. | Exploiting vulnerabilities | CVE-2026-102764 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Proxy tunneler | | Covert tunnelling, internal pivoting | BeyondTrust Remote Support ≤26.2.3 |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| ARMORY CASTLE | | | https://www.beyondtrust.com/trust-center/security-advisories/bt26-05 |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| privcollect | privcollect is a Python credential stealer delivered through a supply-chain compromise of LiteLLM 1.107.0 on October 21, 2026. Using stolen GitHub OAuth tokens, attackers built the release from a lookalike repository (Berri-AI/litellm). The package drops startup hooks that run on every Python launch. They steal browser, cloud, CI/CD, SSH, and AI tool credentials, along with process environment variables and LiteLLM proxy API keys. The stolen data is encrypted and exfiltrated to www.litellm[.]dev. A secondary loader polls a GitHub dead drop hourly to fetch and run remote code. | Software supply-chain compromise | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Credential stealer | | Credential Theft, Data Exfiltration, API Key Theft | LiteLLM (BerriAI) version 1.107.0 |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>SafePay</td><td rowspan="6">SafePay is a ransomware operation active since August 2024 and among the most active of 2026. It has hit at least 600 victims across critical infrastructure sectors in North America, South America, Europe and Australia. It steals data before encryption, then encrypts files with a hybrid of ChaCha20 and RSA and appends the .SafePay extension. Before encrypting, it stops Volume Shadow Copy and factory-resets NAS backup devices.</td><td>Stolen credentials, edge-device exploits</td><td>CVE-2020-3259<br>CVE-2023-20269<br>CVE-2023-27532<br>CVE-2024-40711<br>CVE-2024-40766</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Ransomware</td><td rowspan="3">Data theft, encryption, backup destruction</td><td>Cisco ASA & FTD, Veeam Backup & Replication, SonicWall SonicOS</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINKS</td></tr>
<tr><td>-</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-info-disclose-9eJtycMB, https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC, https://www.veeam.com/kb4424, https://www.veeam.com/kb4649, https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| Sirius Backdoor | Sirius Backdoor is a Windows backdoor built with Microsoft Visual C++ that gives attackers remote control of an infected machine. It keeps its settings either in the file's resource section or in its own memory. Once running, it checks the victim's computer to learn what it is and how well it is protected. It creates a lasting ID for the machine from the disk serial number and computer name. It also collects the CPU, GPU, RAM, screen size, and the user's privilege level. | Phishing | - |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Backdoor | | System Compromise | Windows |
| **ASSOCIATED ACTOR** | | | **PATCH LINK** |
| - | | | - |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

<table>
<tr><th>NAME</th><th>OVERVIEW</th><th>DELIVERY METHOD</th><th>TARGETED CVE</th></tr>
<tr><td>XMRig</td><td rowspan="6">XMRig is an open-source, cross-platform Monero (XMR) cryptocurrency miner that is legitimate software but is one of the most widely abused tools in illicit cryptojacking, as attackers embed it in malware chains to hijack victim CPU resources for mining.</td><td>Exploiting Vulnerability</td><td>CVE-2026-105133<br>CVE-2026-105134<br>CVE-2026-96652<br>CVE-2026-96654<br>CVE-2026-96655<br>CVE-2026-96656</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Cryptominer</td><td rowspan="4">Resource hijacking, persistent access</td><td>Ahsay AhsayCBS, Plex Media Server</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINKS</td></tr>
<tr><td>-</td><td>https://idp3.ahsay.com/idp/Authn/RemoteUser, https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/</td></tr>
</table>

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

| NAME | OVERVIEW | DELIVERY METHOD | TARGETED CVE |
|---|---|---|---|
| myawesome proxy | myawesomeproxy is proxyware that routes third-party traffic through the victim's internet connection. When run, it displays a notice that running it means agreeing to external use of the device's internet traffic. It communicates with proxystream infrastructure. | Exploiting vulnerabilities | CVE-2026-96652<br>CVE-2026-96654<br>CVE-2026-96655<br>CVE-2026-96656 |
| **TYPE** | | **IMPACT** | **AFFECTED PLATFORM** |
| Proxyware | | Bandwidth hijacking, victim IP abused to relay traffic, harder attribution | Plex Media Server |
| **ASSOCIATED ACTOR** | | | **PATCH LINKS** |
| - | | | https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319, https://www.plex.tv/media-server-downloads/ |

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

# Adversaries in Action

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
|  UTA0576 | - | All | Worldwide |
| | **MOTIVE** | | |
| | Information Theft | | |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOM WARE** | **AFFECTED PRODUCT** |
| | CVE-2026-104935 | - | Ivanti Connect Secure |
| **TTPs** | | | |
| TA0001: Initial Access, TA0002: Execution, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1059.006: Python, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1055.009: Proc Memory, T1070: Indicator Removal, T1070.002: Clear Linux or Mac System Logs, T1070.004: File Deletion, T1036: Masquerading, T1036.005: Match Legitimate Name or Location, T1564: Hide Artifacts, T1564.001: Hidden Files and Directories, T1140: Deobfuscate/Decode Files or Information, T1552: Unsecured Credentials, T1552.001: Credentials In Files, T1040: Network Sniffing, T1110: Brute Force, T1110.003: Password Spraying, T1087: Account Discovery, T1087.002: Domain Account, T1016: System Network Configuration Discovery, T1005: Data from Local System, T1560: Archive Collected Data, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1041: Exfiltration Over C2 Channel | | |

| NAME | ORIGIN | TARGETED INDUSTRIES | TARGETED REGIONS |
|---|---|---|---|
| <br>TraderTraitor (also tracked as Lazarus, Pressure Chollima, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Hidden Cobra, Appleworm, APT-C-26, ATK 3, SectorA01, ITG03, TA404, DEV-0139, Guardians of Peace, Gods Apostles, Gods Disciples, UNC577, UNC2970, UNC4034, UNC4736, UNC4899, Diamond Sleet, Citrine Sleet, Jade Sleet, Gleaming Pisces, Slow Pisces, PUKCHONG) | North Korea<br>**MOTIVE**<br>Financial Gain | Cryptocurrency, Fintech, Venture Capital, IT Services, Cloud Identity and SaaS Providers | Worldwide |
| | **TARGETED CVE** | **ASSOCIATED ATTACKS/RANSOMWARE** | **AFFECTED PRODUCT** |
| | - | FLATROOF, ROOFDECK | macOS, Windows, Linux |

**TTPs**

TA0042: Resource Development; TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0008: Lateral Movement; TA0009: Collection; TA0011: Command and Control; TA0010: Exfiltration; TA0040: Impact; T1583: Acquire Infrastructure; T1608: Stage Capabilities; T1566: Phishing; T1195: Supply Chain Compromise; T1199: Trusted Relationship; T1204: User Execution; T1059: Command and Scripting Interpreter; T1546: Event Triggered Execution; T1543: Create or Modify System Process; T1547: Boot or Logon Autostart Execution; T1098: Account Manipulation; T1036: Masquerading; T1027: Obfuscated Files or Information; T1140: Deobfuscate/Decode Files or Information; T1553: Subvert Trust Controls; T1055: Process Injection; T1070: Indicator Removal; T1555: Credentials from Password Stores; T1552: Unsecured Credentials; T1539: Steal Web Session Cookie; T1082: System Information Discovery; T1057: Process Discovery; T1083: File and Directory Discovery; T1518: Software Discovery; T1217: Browser Information Discovery; T1580: Cloud Infrastructure Discovery; T1550: Use Alternate Authentication Material; T1115: Clipboard Data; T1560: Archive Collected Data; T1071: Application Layer Protocol; T1102: Web Service; T1008: Fallback Channels; T1573: Encrypted Channel; T1105: Ingress Tool Transfer; T1567: Exfiltration Over Web Service; T1041: Exfiltration Over C2 Channel; T1657: Financial Theft; T1583.001: Domains; T1608.001: Upload Malware; T1566.003: Spearphishing via Service; T1195.001: Compromise Software Dependencies and Development Tools; T1204.002: Malicious File; T1059.004: Unix Shell; T1059.006: Python; T1059.007: JavaScript; T1546.004: Unix Shell Configuration Modification; T1543.001: Launch Agent; T1543.002: Systemd Service; T1547.001: Registry Run Keys / Startup Folder; T1098.005: Device Registration; T1036.005: Match Legitimate Resource Name or Location; T1036.008: Masquerade File Type; T1027.009: Embedded Payloads; T1027.013: Encrypted/Encoded File; T1553.001: Gatekeeper Bypass; T1553.002: Code Signing; T1055.012: Process Hollowing; T1070.004: File Deletion; T1555.001: Keychain; T1555.003: Credentials from Web Browsers; T1555.004: Windows Credential Manager; T1552.003: Shell History; T1518.001: Security Software Discovery; T1550.004: Web Session Cookie; T1560.001: Archive via Utility; T1071.001: Web Protocols; T1102.001: Dead Drop Resolver; T1102.002: Bidirectional Communication; T1573.001: Symmetric Cryptography

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="5"><br>ARMORY CASTLE (aka UNC5221, WARP PANDA)</td><td>China (suspected)</td><td rowspan="3">-</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Cyber espionage</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2026-102764</td><td>SAWFLY, BARECLAW</td><td>BeyondTrust Remote Support</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0042: Resource Development, TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0009: Collection, TA0011: Command and Control, T1584: Compromise Infrastructure, T1584.008: Network Devices, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1505: Server Software Component, T1505.003: Web Shell, T1098: Account Manipulation, T1548: Abuse Elevation Control Mechanism, T1548.001: Setuid and Setgid, T1078: Valid Accounts, T1070: Indicator Removal, T1070.002: Clear Linux or Mac System Logs, T1070.004: File Deletion, T1555: Credentials from Password Stores, T1005: Data from Local System, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1573: Encrypted Channel, T1090: Proxy, T1572: Protocol Tunneling, T1105: Ingress Tool Transfer, T1219: Remote Access Tools, T1219.002: Remote Desktop Software</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"><br>Lazarus</td><td>North Korea</td><td rowspan="3">Government, financial, logistics, airports, manufacturing, and online transaction platforms</td><td rowspan="3">USA, Japan, Thailand, Indonesia, South Korea, Australia, Taiwan, India, Singapore, UAE, Saudi Arabia, and the EU</td></tr>
<tr><th>MOTIVE</th></tr>
<tr><td>Information theft and espionage, Sabotage and destruction, Financial crime</td></tr>
<tr><th>TARGETED CVE</th><th>ASSOCIATED ATTACKS/RANSOM WARE</th><th>AFFECTED PRODUCT</th></tr>
<tr><td>CVE-2026-109618<br>CVE-2026-109619</td><td>-</td><td>PHP</td></tr>
<tr><th colspan="4">TTPs</th></tr>
<tr><td colspan="4">TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0007: Discovery, TA0006: Credential Access, TA0009: Collection, TA0005: Defense Evasion, TA0043: Reconnaissance, TA0042: Resource Development, TA0011: Command and Control, TA0008: Lateral Movement, TA0010: Exfiltration, TA0040: Impact, T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1059.004: Unix Shell, T1505: Server Software Component, T1505.003: Web Shell, T1098: Account Manipulation, T1098.004: SSH Authorized Keys, T1053: Scheduled Task/Job, T1053.003: Cron, T1033: System Owner/User Discovery, T1212: Exploitation for Credential Access, T1552: Unsecured Credentials, T1552.001: Credentials In Files, T1005: Data from Local System, T1211: Exploitation for Defense Evasion, T1595: Active Scanning, T1595.002: Vulnerability Scanning, T1590: Gather Victim Network Information, T1588: Obtain Capabilities, T1588.005: Exploits, T1608: Stage Capabilities, T1583: Acquire Infrastructure, T1583.004: Server, T1105: Ingress Tool Transfer, T1210: Exploitation of Remote Services, T1041: Exfiltration Over C2 Channel, T1496: Resource Hijacking, T1486: Data Encrypted for Impact</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"><br>CL-STA-0954 (aka UNC5820)</td><td>-</td><td rowspan="2">Telecommunications, Managed Service Providers</td><td rowspan="2">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information Theft</td><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-61624<br>CVE-2024-47575</td><td>PEERSTITCH</td><td>Fortinet FortiManager, Fortinet FortiGate, Fortinet FortiOS, Fortinet FortiPAM, Fortinet FortiProxy, Fortinet FortiSwitchManager</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access, TA0002: Execution, TA0003: Persistence, TA0004: Privilege Escalation, TA0005: Defense Evasion, TA0006: Credential Access, TA0007: Discovery, TA0008: Lateral Movement, TA0009: Collection, TA0011: Command and Control, TA0010: Exfiltration, T1190: Exploit Public-Facing Application, T1133: External Remote Services, T1078: Valid Accounts, T1078.003: Local Accounts, T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1543: Create or Modify System Process, T1068: Exploitation for Privilege Escalation, T1055: Process Injection, T1055.008: Ptrace System Calls, T1562: Impair Defenses, T1562.001: Disable or Modify Tools, T1070: Indicator Removal, T1070.002: Clear Linux or Mac System Logs, T1070.004: File Deletion, T1036: Masquerading, T1014: Rootkit, T1211: Exploitation for Defense Evasion, T1110: Brute Force, T1110.002: Password Cracking, T1040: Network Sniffing, T1552: Unsecured Credentials, T1552.001: Credentials In Files, T1649: Steal or Forge Authentication Certificates, T1046: Network Service Discovery, T1021: Remote Services, T1005: Data from Local System, T1074: Data Staged, T1074.001: Local Data Staging, T1602: Data from Configuration Repository, T1071: Application Layer Protocol, T1071.001: Web Protocols, T1105: Ingress Tool Transfer, T1219: Remote Access Tools, T1205: Traffic Signaling, T1008: Fallback Channels, T1041: Exfiltration Over C2 Channel</td></tr>
</table>

# MITRE ATT&CK TTPS

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0001: Initial Access | T1078: Valid Accounts | T1078.003: Local Accounts |
| | | T1078.004: Cloud Accounts |
| | T1133: External Remote Services | |
| | T1189: Drive-by Compromise | |
| | T1190: Exploit Public-Facing Application | |
| | T1195: Supply Chain Compromise | T1195.001: Compromise Software Dependencies and Development Tools |
| | | T1195.002: Compromise Software Supply Chain |
| | T1199: Trusted Relationship | |
| | T1566: Phishing | T1566.001: Spearphishing Attachment |
| | | T1566.002: Spearphishing Link |
| | | T1566.003: Spearphishing via Service |
| TA0002: Execution | T1047: Windows Management Instrumentation | |
| | T1053: Scheduled Task/Job | T1053.003: Cron |
| | | T1053.005: Scheduled Task |
| | T1059: Command and Scripting Interpreter | T1059.001: PowerShell |
| | | T1059.003: Windows Command Shell |
| | | T1059.004: Unix Shell |
| | | T1059.005: Visual Basic |
| | | T1059.006: Python |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0002: Execution | T1059: Command and Scripting Interpreter | T1059.007: JavaScript |
| | | T1059.008: Network Device CLI |
| | T1072: Software Deployment Tools | |
| | T1106: Native API | |
| | T1129: Shared Modules | |
| | T1203: Exploitation for Client Execution | |
| | T1204: User Execution | T1204.002: Malicious File |
| | T1569: System Services | T1569.002: Service Execution |
| TA0003: Persistence | T1037: Boot or Logon Initialization Scripts | T1037.001: Logon Script (Windows) |
| | | T1037.004: RC Scripts |
| | T1053: Scheduled Task/Job | T1053.003: Cron |
| | | T1053.005: Scheduled Task |
| | T1078: Valid Accounts | T1078.003: Local Accounts |
| | | T1078.004: Cloud Accounts |
| | T1098: Account Manipulation | T1098.004: SSH Authorized Keys |
| | | T1098.005: Device Registration |
| | T1133: External Remote Services | |
| | T1136: Create Account | T1136.003: Cloud Account |
| | T1205: Traffic Signaling | |
| | T1505: Server Software Component | T1505.003: Web Shell |
| | T1543: Create or Modify System Process | T1543.001: Launch Agent |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0003: Persistence | T1543: Create or Modify System Process | T1543.002: Systemd Service |
| | | T1543.003: Windows Service |
| | T1546: Event Triggered Execution | T1546.004: Unix Shell Configuration Modification |
| | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder |
| | | T1547.005: Security Support Provider |
| | T1556: Modify Authentication Process | T1556.003: Pluggable Authentication Modules |
| | | T1556.004: Network Device Authentication |
| | T1574: Hijack Execution Flow | T1574.002: DLL Side-Loading |
| | | T1574.006: Dynamic Linker Hijacking |
| TA0004: Privilege Escalation | T1037: Boot or Logon Initialization Scripts | T1037.001: Logon Script (Windows) |
| | | T1037.004: RC Scripts |
| | T1053: Scheduled Task/Job | T1053.003: Cron |
| | | T1053.005: Scheduled Task |
| | T1055: Process Injection | T1055.004: Asynchronous Procedure Call |
| | | T1055.008: Ptrace System Calls |
| | | T1055.009: Proc Memory |
| | | T1055.012: Process Hollowing |
| | T1068: Exploitation for Privilege Escalation | |
| | T1078: Valid Accounts | T1078.003: Local Accounts |
| | | T1078.004: Cloud Accounts |
| | T1098: Account Manipulation | T1098.004: SSH Authorized Keys |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0004: Privilege Escalation | T1098: Account Manipulation | T1098.005: Device Registration |
| | T1134: Access Token Manipulation | T1134.001: Token Impersonation/Theft |
| | T1543: Create or Modify System Process | T1543.002: Systemd Service |
| | | T1543.003: Windows Service |
| | T1546: Event Triggered Execution | T1546.004: Unix Shell Configuration Modification |
| | T1547: Boot or Logon Autostart Execution | T1547.001: Registry Run Keys / Startup Folder |
| | | T1547.005: Security Support Provider |
| | T1548: Abuse Elevation Control Mechanism | T1548.001: Setuid and Setgid |
| | | T1548.002: Bypass User Account Control |
| | | T1548.003: Sudo and Sudo Caching |
| | T1574: Hijack Execution Flow | T1574.002: DLL Side-Loading |
| | | T1574.006: Dynamic Linker Hijacking |
| | T1611: Escape to Host | |
| TA0005: Defense Evasion | T1014: Rootkit | |
| | T1027: Obfuscated Files or Information | T1027.002: Software Packing |
| | | T1027.009: Embedded Payloads |
| | | T1027.013: Encrypted/Encoded File |
| | T1036: Masquerading | T1036.003: Rename System Utilities |
| | | T1036.004: Masquerade Task or Service |
| | | T1036.005: Match Legitimate Name or Location |
| | T1055: Process Injection | T1055.004: Asynchronous Procedure Call |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0005: Defense Evasion | T1055: Process Injection | T1055.008: Ptrace System Calls |
| | | T1055.009: Proc Memory |
| | | T1055.012: Process Hollowing |
| | T1070: Indicator Removal | T1070.001: Clear Windows Event Logs |
| | | T1070.002: Clear Linux or Mac System Logs |
| | | T1070.004: File Deletion |
| | T1078: Valid Accounts | T1078.003: Local Accounts |
| | | T1078.004: Cloud Accounts |
| | T1112: Modify Registry | |
| | T1127: Trusted Developer Utilities Proxy Execution | T1127.001: MSBuild |
| | T1134: Access Token Manipulation | T1134.001: Token Impersonation/Theft |
| | T1140: Deobfuscate/Decode Files or Information | |
| | T1205: Traffic Signaling | |
| | T1211: Exploitation for Defense Evasion | |
| | T1218: System Binary Proxy Execution | T1218.010: Regsvr32 |
| | T1222: File and Directory Permissions Modification | T1222.002: Linux and Mac File and Directory Permissions Modification |
| | T1480: Execution Guardrails | |
| | T1497: Virtualization/Sandbox Evasion | T1497.001: System Checks |
| | T1548: Abuse Elevation Control Mechanism | T1548.001: Setuid and Setgid |
| | | T1548.002: Bypass User Account Control |
| | | T1548.003: Sudo and Sudo Caching |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0005: Defense Evasion | T1550: Use Alternate Authentication Material | T1550.001: Application Access Token |
| | | T1550.004: Web Session Cookie |
| | T1553: Subvert Trust Controls | T1553.001: Gatekeeper Bypass |
| | | T1553.002: Code Signing |
| | | T1553.005: Mark-of-the-Web Bypass |
| | T1556: Modify Authentication Process | T1556.003: Pluggable Authentication Modules |
| | | T1556.004: Network Device Authentication |
| | T1562: Impair Defenses | T1562.001: Disable or Modify Tools |
| | | T1562.002: Disable Windows Event Logging |
| | | T1562.004: Disable or Modify System Firewall |
| | | T1562.006: Indicator Blocking |
| | T1564: Hide Artifacts | T1564.001: Hidden Files and Directories |
| | T1574: Hijack Execution Flow | T1574.002: DLL Side-Loading |
| | | T1574.006: Dynamic Linker Hijacking |
| | T1620: Reflective Code Loading | |
| | T1622: Debugger Evasion | |
| TA0006: Credential Access | T1003: OS Credential Dumping | T1003.006: DCSync |
| | T1040: Network Sniffing | |
| | T1056: Input Capture | T1056.001: Keylogging |
| | T1110: Brute Force | T1110.002: Password Cracking |
| | | T1110.003: Password Spraying |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0006: Credential Access | T1212: Exploitation for Credential Access | |
| | T1528: Steal Application Access Token | |
| | T1539: Steal Web Session Cookie | |
| | T1552: Unsecured Credentials | T1552.001: Credentials In Files |
| | | T1552.002: Credentials in Registry |
| | | T1552.004: Private Keys |
| | | T1552.005: Cloud Instance Metadata API |
| | | T1552.007: Container API |
| | T1555: Credentials from Password Stores | T1555.001: Keychain |
| | | T1555.003: Credentials from Web Browsers |
| | | T1555.004: Windows Credential Manager |
| | | T1555.005: Password Managers |
| | T1556: Modify Authentication Process | T1556.003: Pluggable Authentication Modules |
| | | T1556.004: Network Device Authentication |
| | T1557: Adversary-in-the-Middle | |
| | T1649: Steal or Forge Authentication Certificates | |
| TA0007: Discovery | T1012: Query Registry | |
| | T1016: System Network Configuration Discovery | T1016.001: Internet Connection Discovery |
| | T1033: System Owner/User Discovery | |
| | T1040: Network Sniffing | |
| | T1046: Network Service Discovery | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0007: Discovery | T1057: Process Discovery | |
| | T1082: System Information Discovery | |
| | T1083: File and Directory Discovery | |
| | T1087: Account Discovery | T1087.001: Local Account |
| | | T1087.002: Domain Account |
| | T1124: System Time Discovery | |
| | T1135: Network Share Discovery | |
| | T1217: Browser Information Discovery | |
| | T1482: Domain Trust Discovery | |
| | T1497: Virtualization/Sandbox Evasion | T1497.001: System Checks |
| | T1518: Software Discovery | T1518.001: Security Software Discovery |
| | T1580: Cloud Infrastructure Discovery | |
| | T1614: System Location Discovery | T1614.001: System Language Discovery |
| | T1622: Debugger Evasion | |
| TA0008: Lateral Movement | T1021: Remote Services | T1021.001: Remote Desktop Protocol |
| | | T1021.002: SMB/Windows Admin Shares |
| | | T1021.004: SSH |
| | | T1021.006: Windows Remote Management |
| | | T1021.007: Cloud Services |
| | T1072: Software Deployment Tools | |
| | T1210: Exploitation of Remote Services | |

| Tactic | Technique | Sub-technique |
|---|---|---|
| **TA0008: Lateral Movement** | T1550: Use Alternate Authentication Material | T1550.001: Application Access Token |
| | | T1550.004: Web Session Cookie |
| **TA0009: Collection** | T1005: Data from Local System | |
| | T1039: Data from Network Shared Drive | |
| | T1056: Input Capture | T1056.001: Keylogging |
| | T1074: Data Staged | T1074.001: Local Data Staging |
| | T1113: Screen Capture | |
| | T1114: Email Collection | T1114.001: Local Email Collection |
| | | T1114.003: Email Forwarding Rule |
| | T1115: Clipboard Data | |
| | T1123: Audio Capture | |
| | T1125: Video Capture | |
| | T1557: Adversary-in-the-Middle | |
| | T1560: Archive Collected Data | T1560.001: Archive via Utility |
| | | T1560.002: Archive via Library |
| | T1602: Data from Configuration Repository | |
| **TA0010: Exfiltration** | T1029: Scheduled Transfer | |
| | T1041: Exfiltration Over C2 Channel | |
| | T1048: Exfiltration Over Alternative Protocol | T1048.003: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol |
| | T1567: Exfiltration Over Web Service | T1567.001: Exfiltration to Code Repository |
| | | T1567.002: Exfiltration to Cloud Storage |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0011: Command and Control | T1008: Fallback Channels | |
| | T1071: Application Layer Protocol | T1071.001: Web Protocols |
| | T1090: Proxy | T1090.001: Internal Proxy |
| | T1095: Non-Application Layer Protocol | |
| | T1102: Web Service | T1102.001: Dead Drop Resolver |
| | | T1102.002: Bidirectional Communication |
| | T1105: Ingress Tool Transfer | |
| | T1132: Data Encoding | T1132.001: Standard Encoding |
| | T1205: Traffic Signaling | |
| | T1219: Remote Access Software | |
| | T1571: Non-Standard Port | |
| | T1572: Protocol Tunneling | |
| | T1573: Encrypted Channel | T1573.001: Symmetric Cryptography |
| TA0040: Impact | T1485: Data Destruction | |
| | T1486: Data Encrypted for Impact | |
| | T1489: Service Stop | |
| | T1490: Inhibit System Recovery | |
| | T1496: Resource Hijacking | |
| | T1499: Endpoint Denial of Service | T1499.004: Application or System Exploitation |
| | T1531: Account Access Removal | |
| | T1565: Data Manipulation | T1565.002: Transmitted Data Manipulation |

| Tactic | Technique | Sub-technique |
|---|---|---|
| TA0040: Impact | T1657: Financial Theft | |
| TA0042: Resource Development | T1583: Acquire Infrastructure | T1583.001: Domains |
| | | T1583.004: Server |
| | | T1583.006: Web Services |
| | T1584: Compromise Infrastructure | T1584.001: Domains |
| | | T1584.003: Virtual Private Server |
| | T1587: Develop Capabilities | T1587.001: Malware |
| | | T1587.004: Exploits |
| | T1588: Obtain Capabilities | T1588.002: Tool |
| | | T1588.003: Code Signing Certificates |
| | | T1588.004: Digital Certificates |
| | | T1588.006: Vulnerabilities |
| | T1608: Stage Capabilities | T1608.001: Upload Malware |
| TA0043: Reconnaissance | T1590: Gather Victim Network Information | T1590.002: DNS |
| | T1592: Gather Victim Host Information | |
| | T1595: Active Scanning | T1595.002: Vulnerability Scanning |
| | T1598: Phishing for Information | T1598.002: Spearphishing Attachment |
| | | T1598.004: Spearphishing Voice |

# Top 5 Takeaways

**#1**

In October 2026, **15 zero-day** vulnerabilities surfaced. These zero-days were found across products from **Microsoft Windows, Cisco, Citrix, Fortinet, Ivanti, Palo Alto Networks, BeyondTrust, Arista, Ahsay,** and **PHP**.

**#2**

Malware active in October spanned a broad mix of **Backdoors, Infostealers, Loaders, Web Shells,** and **Proxies**. Key families were **ShelbyLoader, ShelbyC2, ClingSTUN, PEERSTITCH, SAWFLY, BARECLAW, FLATROOF, ROOFDECK, Aoki, privcollect**, and **Sirius**, each representing distinct capabilities ranging from in-memory stealth and developer credential theft to large-scale device and firewall compromise.

**#3**

Beyond the many campaigns with worldwide reach, targeted activity concentrated on the **United Arab Emirates, United Kingdom, United States, Australia,** and **Iraq**. Espionage campaigns, phishing lures, and opportunistic exploitation drove this focus, underscoring that no region remained insulated as adversaries expanded their operations worldwide.

**#4**

**Financial, Telecommunications, Aviation, IT Services, and Technology** sectors absorbed the bulk of targeted activity, with ransomware operations, espionage campaigns, and software supply chain compromises driving operational disruption. Attackers continued refining techniques and expanding pressure across these industries.

**#5**

Activity during the period was dominated by **Armory Castle, TraderTraitor, and CL-STA-0954,** a mix of China-nexus, North Korean, and suspected nation-state groups. Their campaigns combined zero-day exploitation of edge appliances, poisoned developer tooling, and fake job lures, with a clear focus on long-term access and credential theft.

# Recommendations

**Security Teams**

This digest can be used as a guide to help security teams prioritize the **66 significant vulnerabilities** and block the indicators related to the **5 active threat actors, 23 active malware,** and **240 potential MITRE TTPs.**

**Uni5 Users**

This is an actionable threat digest for HivePro Uni5 customers, who can get comprehensive insights into their threat exposure and take action easily through the HivePro Uni5 dashboard by:

• Running a scan to discover the assets impacted by the **66 significant vulnerabilities**

• Testing the efficacy of their security controls by simulating the attacks related to **active threat actors, active malware**, and **potential MITRE TTPs** in Breach and Attack Simulation(BAS).

# Appendix

**Known Exploited Vulnerabilities (KEV):** Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

**Celebrity Vulnerabilities:** Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide malicious actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

**Social engineering:** is an attack that relies on human interaction to persuade people into compromising security. It involves various strategies aimed at extracting specific information or performing illicit activities from a target.

**Supply chain attack:** Also known as a value-chain or third-party attack, occurs when an outside partner or provider with access to your systems and data infiltrates your system. The purpose is to gain access to source codes, development processes, or update mechanisms in order to distribute malware by infecting legitimate programs.

**Eavesdropping:** Often known as sniffing or spying, is a significant risk in cybersecurity. Passwords, credit card information, and other sensitive data are easily stolen during these attacks as they are transmitted from one device to another. This type of network attack often occurs when unsecured networks, such as public Wi-Fi connections or shared electronic devices, are used.

**Glossary:**

**CISA KEV -** Cybersecurity & Infrastructure Security Agency Known Exploited Vulnerabilities
**CVE -** Common Vulnerabilities and Exposures
**CPE -** Common Platform Enumeration
**CWE** - Common Weakness Enumeration

# Indicators of Compromise (IOCs)

| Attack Name | TYPE | VALUE |
|---|---|---|
| Chopper | SHA256 | 13d27ecfbb6b3d55bdabcaa3a2ade83ecfaa3df92dbc22be05e6d9e2d18087b6, dc76d856d42242e58eb8d4b70d5378f42f3ddf0ef7872d2279f2d67c22806e26, 5cc6bc95c584d72cc61842f0ee58f38ac4519ec953a2dff3d37e2e8f389f3d54 |
| CoinMiner | SHA256 | aea991f694911e321b0ab97534f2ad0291c392c0a43dabff664c563618bd036d |
| Looptik | SHA256 | 65a7576c389326b6cdf9c993d0be6e5d50fed9655d1cdf2a3a50f2c21c8ec435 |
| Zimdown2 | SHA256 | bf28f38122bf20d5fac969cc414daa6a890cdea872d389ca93d2092b6b7773cf |
| Zimclient2 | SHA256 | b594a42b8f1c6f090327bb9a3361c2d3515537fb7ac8da6b9061b9a3f330e159 |
| ShelbyC2 | Filename | RuntimeBrokerApi.dll |
| PsProxy | Filename | PsProxy.dll |
| | SHA256 | 3fd810a3aa0039993393741b32287c367a9a5037a41e826906440887cdd3ed13 |
| ShelbyLoader | Filename | RuntimeBroker.dll, RuntimeBroker.exe.config, DubaiAirport_Carrers_IT_Test.zip, FlightManager.csproj |
| | SHA256 | 53f35e49eb9b271fd8cbcd3daacb525328dbf159a03dbd1c7adebe0363daa402 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| ShelbyLoader | SHA256 | 6e7d9b33f1e72ea1ede71373a604ecdb060dab7d42055179c1eede9ecd1fd239, f5b12772db6817f7a765a6fe7565fd3d4f87edc28e42fe3ec0244a372a410fc9 |
| Blackwood | IPv4 | 91[.]107[.]156[.]29, 65[.]109[.]214[.]145, 87[.]248[.]129[.]239, |
| | IPv4:PORT | 65[.]109[.]214[.]145[:]8080 |
| | SHA256 | 76273382e4252c1f60a2251141e108942494409c759358320735891762c0682e, d3561bd4aad003dc3e08157b0891860bb496b80cd6e44901692e08ab1d4e8260, f5ba1645694c62f527ed6ceda8c68a5c3dd92b4032439167e8e937e72803b4bd, 7cc571aca6d8715d9aaad3d83e1bcd30467565d583db1dfe73697c5d00a1f875 |
| Shai-Hulud | SHA256 | 25a0735d0db7dc40e5d45ce42d9c106067e6a66e184d967cfecfab17c3bcb5ef, b50a00900399ba99fb6ce1fc151519cb99d44320ef2a631f2237e1aea0ad6fec |
| ClingSTUN | SHA256 | e6e113783356446aef66e5296db45b244f318292af7cebc2a9bd76f095a95c4c, c1d8e2829ea63b9dc1cf2c3421a5093406adad4d6622e238376e78e908e0e6e8, ec199c78c11040fd3127887222fd75a85e5797bf96aa691a117fdd83dd663d81, dc892f5013edb0aa1e61e808511387373d8d120348b5be0929621d21e6e9946a |
| XMRig | SHA256 | 739f7328a5d0912cace9d289d7f2d295117d74580c08a6a02d72c94cba41416e |

| Attack Name | TYPE | VALUE |
|---|---|---|
| XMRig | SHA256 | fcde8af943753f831219c1d1ff82a425ff27b8c8e72dee6e4d64e95912125804, dd752e32f65f4508f86b1cd1d2795e96614b6e76dd4d1d2a686c0b01b6c69b24, a06b4510e3af4b544e617c5ac30267e33df9fed0c5592231b2a1ab3fefb0d8eb, 3c36581fac391feee2b35b385f423d8502f11a80d65e5f5788df8c22ebfc2f43, d8b9b5a48070d6d3774be3ec176b0cd30b40a4da2779f072243d20bd9fc2901f, 23ee60f1bd28f720527167be17861ff7f369ca89e0b0c3cd29ba3849bc3542ff, 155b5c9a6a8a93f249278f7c46a376abe595ac90ddf4771cf2da47805e54529d, 2d3c618b21a7e2f8bcd735da188e44a7609ff3f204832dd0781cd09e4388c9db |
| FLATROOF | SHA256 | 451b586ec9d3c997b319986a1177829653e8ae641c953c05ede6a38616f2da97 |
| ROOFDECK | SHA256 | e1c71374814e5d907afb913108090b8abf21ae2131c0880f013a3b9108a9d0fc |
| PEERSTITCH | SHA256 | b9fb0b27ddd59b58d3ae53c7227298a3e0de1e6f868b9429ae21533bb9cd1e70 |
| | IPv4 | 23[.]240[.]77[.]233, 47[.]18[.]167[.]159 |
| | URL | hxxp[:]//23[.]240[.]77[.]233[:]8085/pM.js, hxxp[:]//47[.]18[.]167[.]159[:]8085/pM.js |
| Aoki | SHA256 | 752c8e64af60960b85cf00e4bd34eb459e24b7939464f718ec18494df43b4b69 |

| Attack Name | TYPE | VALUE |
|---|---|---|
| Aoki | SHA256 | bf037920d39b85572ec7e53b51f09c28198c2c0afbc7c7d6cf639b1f047caebf,<br>0adc8e83b2416c275b1283916d70568faddeb6d718eb45f9addfb0938db245b3,<br>6655b89b9885483d459c73f2a52e3cec121de5c5956172a8676a0f4c2de94999,<br>780bbdbb119befd4eb16e0c2ec0c64e7bedc1b53ce4f85804aea091a6e3af519,<br>2fb80e2221bd304e7cd5ac04169e71807ad92d19836f1aaf7885295cb90b2d94,<br>73dbac0907e8a092cd978f2787ab1994946f5da1e08f2bdbd05ea52e80cdb896,<br>07bc2e3a1d14743cc44f1dc4c78d15d0f2b458b39fb48422b13df40fc662ba21,<br>c533570fd7cd7eaf5478317b03ea5750d03797aa4d11ebd96555b6cb708c63f2,<br>6350dfee6975a9b159c5a57a3e97f757b0b02fd2dc708016fa6d7270e720c865,<br>36af3acc78058023cdcf9307bc15be640be9425de97e574fdaf42d03d308725b,<br>039240551f88b0064b2615dffdc1321b1e7c58e3f617ac138a65a6d59400b331,<br>0e38bd3c30a4ca08641240ce95b5b6ba593e131213ca1b2a28da4e0385fcabc4,<br>3b4547f0d7549274f366cd9568b3d302c1e80e1b89359da681beb47260ec7975,<br>b590235493487c51f7050b341c9b2450e4f761ad6055207e4f6daf0cecae271c,<br>e374f9ff5094f728528efa566c3de1b7fea7d95f497242a01fffa6c70b5eb768,<br>f779314b1a5a0b297fd4e2a5f9c1e40d387b3e7c401d42324b556a70f813840e |
| SAWFLY | SHA256 | dc14e215269a93fdbc4c1a80b984c23faf7af0911c6dbb85309796a6f2ae95fb |
| | File Name | mangoapi.php |

| Attack Name | TYPE | VALUE |
|---|---|---|
| SAWFLY | File Path | /%SITE_SERVICE_ACCOUNT%/ingredi/app/laravel/public/mangoapi.php |
| | HTTP POST Parameter | _c94mfe |
| | YARA Rule | G_Hunting_Webshell_SAWFLY_1 |
| BARECLAW | SHA256 | 1f19b9a27d79c11bda00a1e8faf74a7fdd683d38ccef1b60df2fd0307e3aa462 |
| privcollect | SHA256 | 03ac2a8b752605d1d7710979c17ff18b03dd978203ba23ba97fd8ce3d6f897ea, 9dd0a3926f96a37eb86cf1ee2310d9be93139cc4ebef3ef9e2efe9531390be25 |
| SafePay | SHA256 | 921df888aaabcd828a3723f4c9f5fe8b8379c6b7067d16b2ea10152300417eae, 6c1d36df94ebe367823e73ba33cfb4f40756a5e8ee1e30e8f0ae55d47e220a6a, e79608cf1d6b51324c14bef8883054c1238ed5f080222cc464810e6e14adc346, 327b8b61eb446cc4f710771e44484f62b804ae3d262b57a56575053e2df67917, a0dc80a37eb7e2716c02a94adc8df9baedec192a77bde31669faed228d9ff526 |
| | SHA1 | 07353237350c35d6dc2c8f143b649cd07c71f62b, b498a2683640c983bb069fa2ea9e67cef4a3797d, BBFED53E3BB1F306F4DA97D995CF4AE5B73AD081 |
| | IPv4 | 77[.]37[.]49[.]40, 167[.]235[.]225[.]149, 5[.]255[.]11[.]134, 37[.]10[.]71[.]188, 88[.]119[.]167[.]239 |
| | Email | ColinSolomon[@]protonmail[.]com |
| | Filename | locker.dll |

| Attack Name | TYPE | VALUE |
|---|---|---|
| SafePay | Filename | soc.dll, readme_safepay.txt, Socks_werfault.exe, DYRasWtb.exe |
| | Hostname | WIN-SBOE3CPNALE, WIN-3IUUOFVTQAR, WIN-DK18BI83M0S, WIN-I1HRRJHCEIV |
| Sirius Backdoor | SHA256 | d6802fce5b918ed247ba85d6aa0545a8120cfbc3734b1c37794c4e381862d4ee |
| | MD5 | e8b080c276519547e95930ab15028adb |
| myawesomeproxy | SHA256 | e546b10aee5edc754da4f9b0baace00392257121911f630145078eafad1e6bd9 |
| | Domain | proxystream[.]st |

*A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.*

# What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

**November 03, 2026 • 10:15 PM**

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com