Date of Publication
October 19, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

12 to 18 OCTOBER 2026

Table Of Contents

Summary 03

High Level Statistics 04

Insights 05

Targeted Countries 06

Targeted Industries 07

Top MITRE ATT&CK TTPs 07

Attacks Executed 08

Vulnerabilities Exploited 12

Adversaries in Action 24

Recommendations 27

Threat Advisories 28

Appendix 29

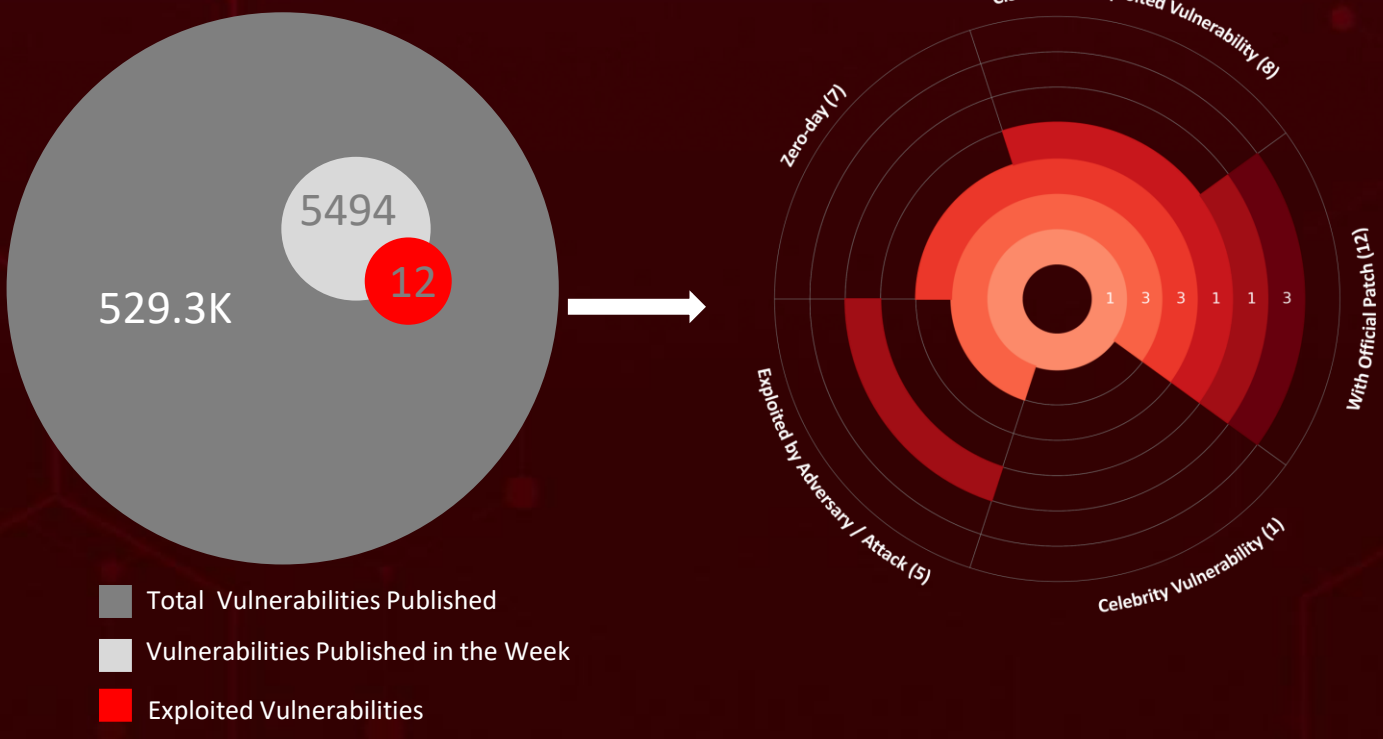
What Next? 31

Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the growing complexity and frequency of global cyber incidents. Over the past week, **four** major attacks were detected, **twelve** vulnerabilities were actively exploited, and **three** threat actor groups were closely monitored, signaling a concerning escalation in malicious activity worldwide.

Among the most significant developments attackers are actively exploiting, AhsayCBS, a backup console used by managed service providers, has two flaws (**CVE-2026-105133** and **CVE-2026-105134**) being exploited together. A broken login check and an OS command flaw let anyone on the internet take full SYSTEM control. Ivanti Connect Secure, a popular SSL VPN gateway, also had a zero-day (**CVE-2026-104935**) that lets attackers run commands without an account or user action. Researchers saw it used as one step in a three-part chain that gives root access on a fully updated device. The attacks are linked to *UTA0576*, a previously unknown actor that used no malware.

Elsewhere, North Korea's **TraderTraitor** group, tied to the USD 1.5 billion Bybit heist, is hiding backdoors (*FLATROOF* and *ROOFDECK*) in fake Terraform add-ons and rigged job-interview coding tests aimed at cloud engineers. These steal passwords, cloud keys, and crypto wallets, and give attackers full remote control. Meanwhile, a suspected nation-state cluster, **CL-STA-0954**, broke into a telecom service provider through the FortiJump flaw in FortiManager. It stole configurations and credentials for more than 500 FortiGate firewalls, then returned to deploy **PEERSTITCH**, a hidden implant that leaves no trace on disk. Together, these incidents show a growing trend of attacks that mix technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered defenses.



High Level Statistics

4
Attacks Executed

12
Vulnerabilities Exploited

3
Adversaries in Action

- XMRig
- FLATROOF
- ROOFDECK
- PEERSTITCH

- CVE-2026-105133
- CVE-2026-105134
- CVE-2026-107406
- CVE-2026-102255
- CVE-2026-104935
- CVE-2026-96951
- CVE-2026-92707
- CVE-2026-108398
- CVE-2026-76519
- CVE-2026-0322
- CVE-2025-61624
- CVE-2024-47575

- UTA0576
- TraderTraitor
- CL-STA-0954

Insights

Every unpatched flaw from the **October 2026 Patch Tuesday** is a gap attackers can study once the fixes are public, so patch fast.

CVE-2026-105133 is a broken login check, and **CVE-2026-105134** runs OS commands, so one flaw opens the door and the other walks right in.

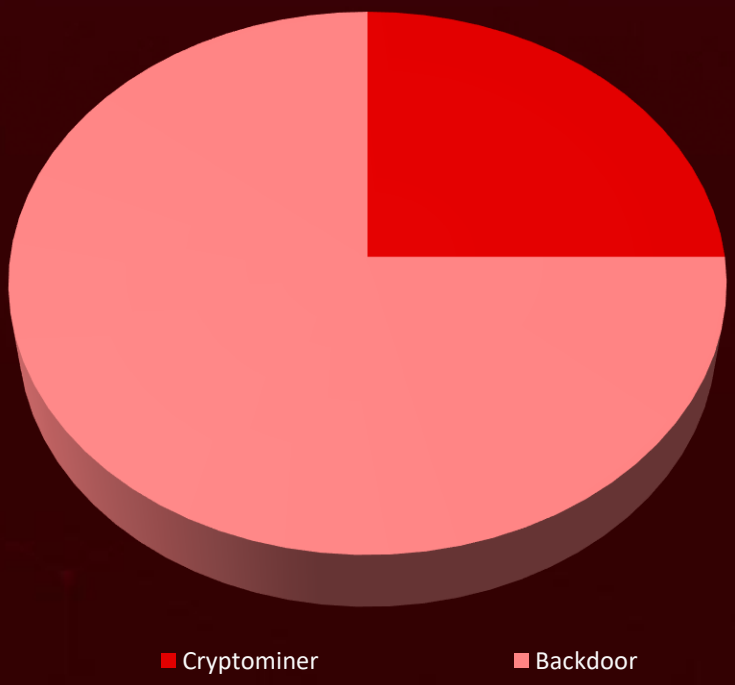
TraderTraitor, the group behind the USD 1.5 billion Bybit heist, is now targeting cloud engineers, shifting the focus from crypto firms to anyone with cloud access.

UTA0576 is a previously unknown actor exploiting **CVE-2026-104935**, so don't assume your known threat lists will catch it.

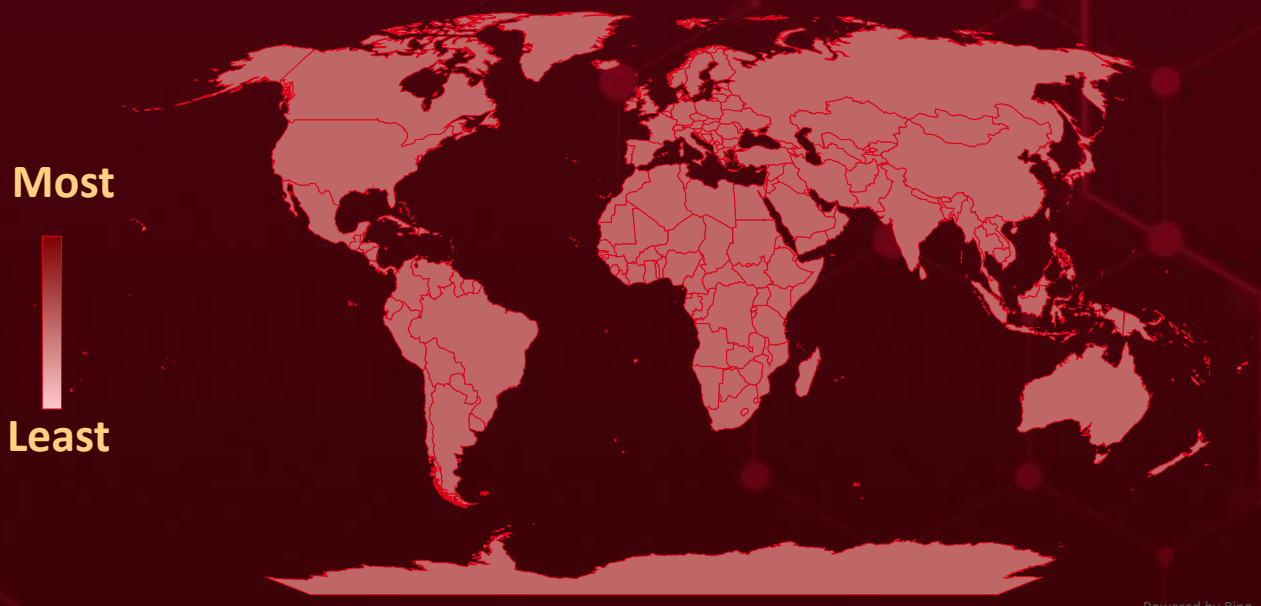
CVE-2026-76519 is a critical Cisco Secure Email Gateway flaw exploited in the wild, so patch now.

CL-STA-0954 broke into a telecom provider through the **FortiJump** flaw, so one central FortiManager can become the way into everything it manages.

Threat Distribution



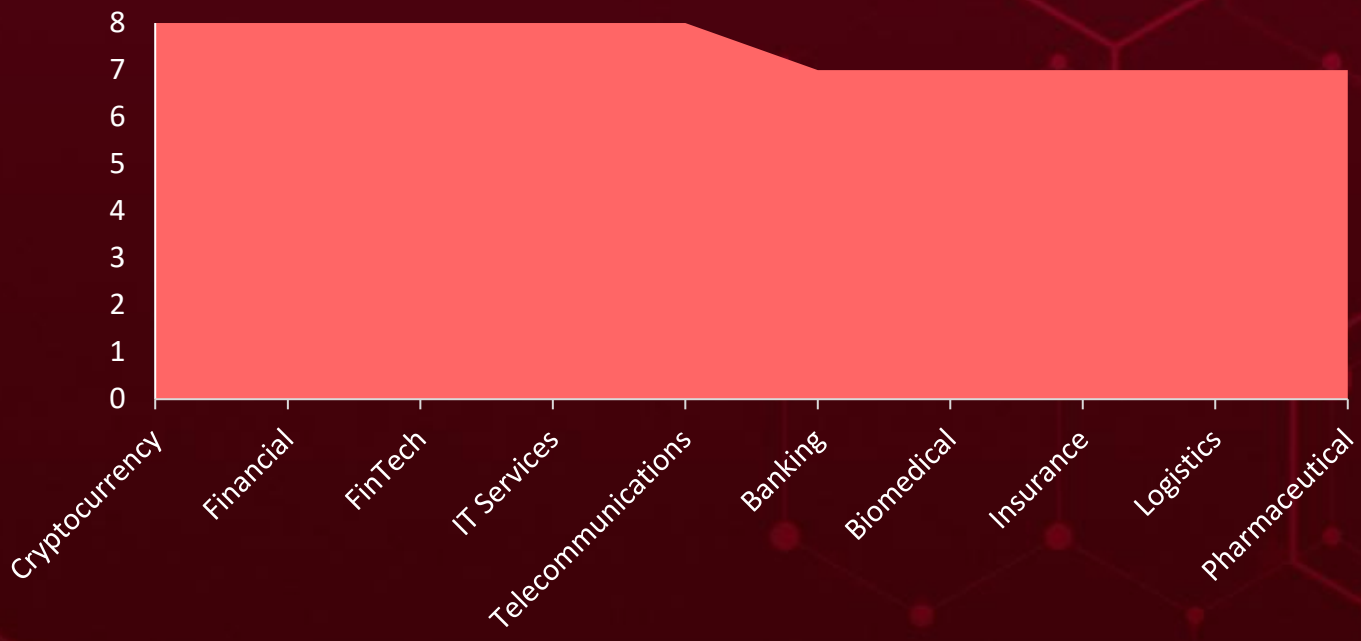
Targeted Countries



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

	Countries		Countries		Countries		Countries
	Ukraine		Belgium		Uruguay		Denmark
	Oman		Togo		Cambodia		Switzerland
	Moldova		Belize		Madagascar		Djibouti
	Brazil		Lithuania		Cameroon		Thailand
	Romania		Benin		Mali		Dominica
	Guinea		Marshall Islands		Canada		Trinidad and Tobago
	Afghanistan		Bhutan		Mauritius		Dominican Republic
	Venezuela		Montenegro		Central African Republic		Tuvalu
	Papua New Guinea		Bolivia		Monaco		Ecuador
	Malaysia		New Zealand		Chad		United Kingdom
	Suriname		Bosnia and Herzegovina		Mozambique		Egypt
	Austria		Pakistan		Chile		Australia
	Namibia		Botswana		Nepal		El Salvador
	Azerbaijan		Poland		China		Luxembourg
	Saudi Arabia		Albania		Niger		Malawi
	Bahamas		Saint Vincent and the Grenadines		Colombia		Eritrea
	Armenia		Brunei		Norway		Maldives
	Bahrain		Sierra Leone		Comoros		Estonia
	Micronesia		Bulgaria		Palestine State		Malta
	Bangladesh		South Sudan		Congo (Congo-Brazzaville)		Mauritania
	North Korea		Burkina Faso		Peru		Ethiopia
	Barbados		Tajikistan		Costa Rica		
	Russia		Burundi		Qatar		
	Belarus		Turkey		Côte d'Ivoire		
	Solomon Islands		Cabo Verde				

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation	**T1071** Application Layer Protocol	**T1036** Masquerading
T1055 Process Injection	**T1105** Ingress Tool Transfer	**T1071.001** Web Protocols	**T1552** Unsecured Credentials	**T1070** Indicator Removal
T1041 Exfiltration Over C2 Channel	**T1588** Obtain Capabilities	**T1070.004** File Deletion	**T1036.005** Match Legitimate Name or Location	**T1588.006** Vulnerabilities
T1040 Network Sniffing	**T1005** Data from Local System	**T1008** Fallback Channels	**T1211** Exploitation for Defense Evasion	**T1110** Brute Force

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVEs
XMRig	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.	Exploiting Vulnerability	CVE-2026-105133 CVE-2026-105134
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Cryptominer		Resource hijacking, persistent access	Ahsay AhsayCBS
ASSOCIATED ACTOR			**PATCH LINK**
-			https://idp3.ahsay.com/idp/Authn/RemoteUser

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>FLATROOF</td><td rowspan="6">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.</td><td>Trojanized Terraform</td><td>-</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Backdoor</td><td rowspan="3">Credential Theft, Cookie Theft, Wallet Theft, Data Exfiltration</td><td>macOS, Windows, Linux</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>TraderTraitor</td><td>-</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">451b586ec9d3c997b319986a1177829653e8ae641c953c05ede6a38616f2da97</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
ROOFDECK	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.	FLATROOF drops ROOFDECK as the final stage	-
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Backdoor		System Discovery, Command Execution, Reverse Shell	macOS, Windows, Linux
ASSOCIATED ACTOR			**PATCH LINK**
TraderTraitor			-
IOC TYPE	**VALUE**		
SHA256	e1c71374814e5d907afb913108090b8abf21ae2131c0880f013a3b9108a9d0fc		

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>PEERSTITCH</td><td rowspan="6">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.</td><td>Exploiting Vulnerability</td><td>CVE-2025-61624
CVE-2024-47575</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Backdoor</td><td rowspan="3">Stealthy persistent firewall compromise.</td><td>Fortinet FortiManager, Fortinet FortiGate, Fortinet FortiOS, Fortinet FortiPAM, Fortinet FortiProxy, Fortinet FortiSwitchManager</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINKS</td></tr>
<tr><td>CL-STA-0954</td><td>https://fortiguard.fortinet.com/psirt/FG-IR-26-122, https://www.fortiguard.com/psirt/FG-IR-24-423</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">b9fb0b27ddd59b58d3ae53c7227298a3e0de1e6f868b9429ae21533bb9cd1e70</td></tr>
</table>

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

Vulnerabilities Exploited

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>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-107406		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)	-
	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:*:*:*:*:*:*:*:*:*	-
Citrix NetScaler ADC and NetScaler Gateway Memory Overflow Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-119	T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service	https://support.citrix.com/external/article/CTX697191/citrix-netscaler-adc-and-citrix-netscale.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-2026-102255</td><td></td><td rowspan="2">SonicWall SMA 1000 Series - 6210, 7210, 8200v (platform-hotfix 12.4.3-03526 and earlier; 12.5.0-02952 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:sonicwall:sma_1000:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">SonicWall SMA 1000 WorkPlace Pre-Authentication Server-Side Request Forgery Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-918
CWE-441</td><td>T1190: Exploit Public-Facing Application</td><td>https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0017</td></tr>
</table>

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

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

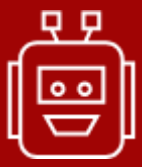
<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2026-76519</td><td></td><td rowspan="2">Cisco Secure Email Gateway (AsyncOS 15.5 before 15.5.5-014, 16.0 all releases, 16.5 before 16.5.0-780; Content Scanner Tools before 25.3.0.5525)</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:cisco:secure_email_gateway:*:*:*:*:*:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="3">Cisco Secure Email Gateway Relative Path Traversal Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td>CWE-23</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkjxp</td></tr>
</table>

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

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

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2024-47575	FortiJump ZERO-DAY	Fortinet FortiManager	CL-STA-0954
		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

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			

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">
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)</td><td>North Korea</td><td rowspan="3">Cryptocurrency, Fintech, Venture Capital, IT Services, Cloud Identity and SaaS Providers</td><td rowspan="3">Worldwide</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial Gain</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>FLATROOF, ROOFDECK</td><td>macOS, Windows, Linux</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">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</td></tr>
</table>

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4">
CL-STA -0954 (aka UNC5820)</td><td>-
MOTIVE
Information Theft</td><td>Telecommunications, Managed Service Providers</td><td>Worldwide</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOM WARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>CVE-2025-61624
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>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **twelve exploited vulnerabilities** and block the indicators related to the threat actors **UTA0576, TraderTraitor, CL-STA-0954,** and malware **XMRig, FLATROOF, ROOFDECK,** and **PEERSTITCH.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **twelve exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating attacks related to the threat actors **TraderTraitor, CL-STA-0954,** and malware **FLATROOF, ROOFDECK,** in Breach and Attack Simulation(BAS).

Threat Advisories

AhsayCBS Zero-Days Turn MSPs Into Crypto Mines

Critical NetScaler SAML Flaw Opens Path to Remote Code Execution

SonicWall SMA 1000 Flaw Turns the Gateway Inward

Ivanti Connect Secure Zero-Day Hands Attackers Root Without a Login

Microsoft’s October 2026 Patch Tuesday - Priority Fixes

CVE-2026-76519: Cisco Email Gateway Zero-Day Exploited for Root Access

TraderTraitor Plants Backdoors in the Cloud Engineer's Toolbox

PAN-OS Management Interface Flaw Exploited for Root-Level Code Execution

PEERSTITCH: The FortiGate Implant That Hides Inside Trusted Processes

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 threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
XMRig	SHA256	739f7328a5d0912cace9d289d7f2d295117d74580c08a6a02d72c94cba41416e, fcde8af943753f831219c1d1ff82a425ff27b8c8e72dee6e4d64e95912125804, dd752e32f65f4508f86b1cd1d2795e96614b6e76dd4d1d2a686c0b01b6c69b24, a06b4510e3af4b544e617c5ac30267e33df9fed0c5592231b2a1ab3fefb0d8eb, 3c36581fac391feee2b35b385f423d8502f11a80d65e5f5788df8c22ebfc2f43, d8b9b5a48070d6d3774be3ec176b0cd30b40a4da2779f072243d20bd9fc2901f, 23ee60f1bd28f720527167be17861ff7f369ca89e0b0c3cd29ba3849bc3542ff, 155b5c9a6a8a93f249278f7c46a376abe595ac90ddf4771cf2da47805e54529d
FLATROOF	SHA256	451b586ec9d3c997b319986a1177829653e8ae641c953c05ede6a38616f2da97

Attack Name	TYPE	VALUE
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

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

October 19, 2026 • 10:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com