Date of Publication
November 2, 2026

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

26 OCTOBER to 01 NOVEMBER 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 11

Adversaries in Action 20

Recommendations 21

Threat Advisories 22

Appendix 23

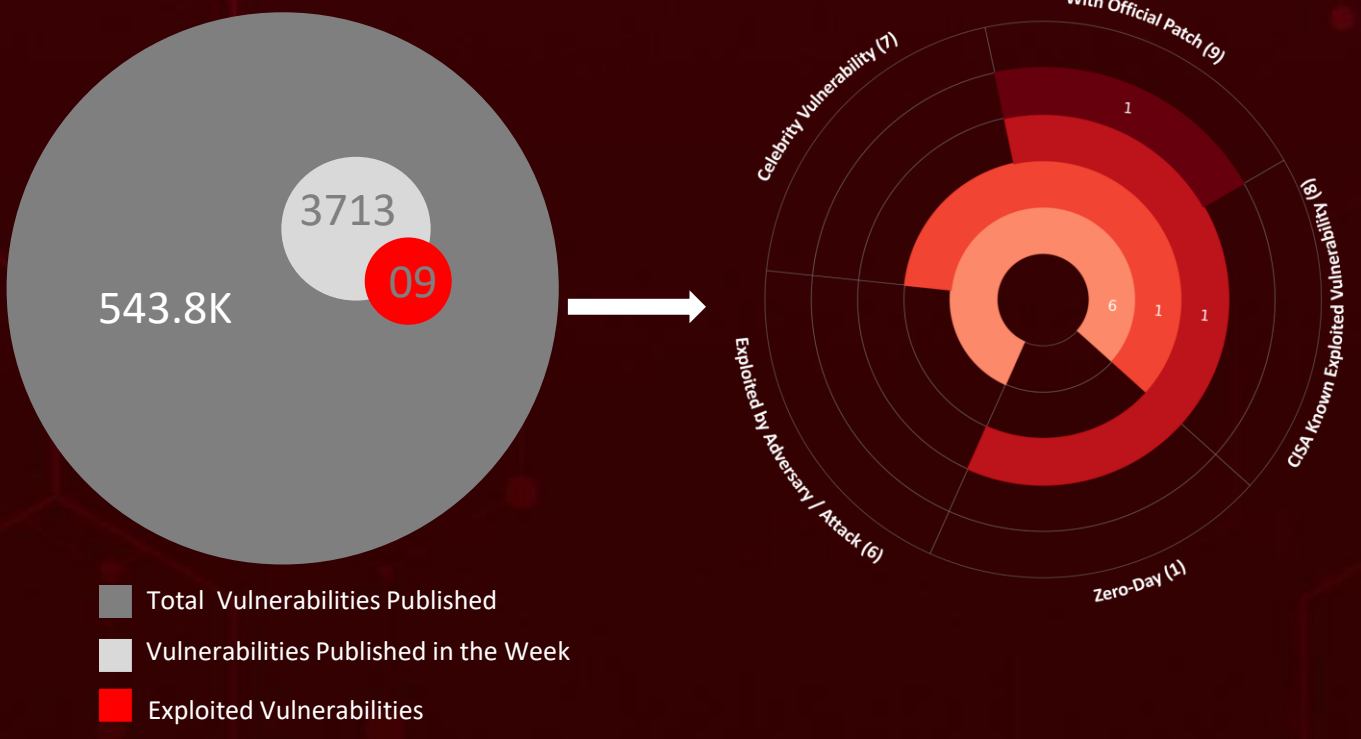
What Next? 24

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, **three** major attacks were detected, **nine** vulnerabilities were actively exploited, and **one** threat actor group was closely monitored, signaling a concerning escalation in malicious activity worldwide.

Leading the week's developments, **Plex2Shell** chains four Plex Media Server flaws (*CVE-2026-96652*, *CVE-2026-96654*, *CVE-2026-96655*, and *CVE-2026-96656*) to give unauthenticated attackers full code execution. They reach internal functions, steal the owner's administrator token, and drop a malicious library into the Codecs directory. Attackers are now mass-exploiting unpatched, internet-facing servers to deploy *XMRig* miners and *myawesomeproxy* proxyware, turning victims into paid relay nodes with a foothold in their networks. Meanwhile, Cisco disclosed **CVE-2026-76418**, a high-severity zero-day in the Remote Access SSL VPN service of Cisco Secure Firewall ASA and FTD software. A single crafted request from an unauthenticated attacker can force the firewall to reload, knocking the device offline and cutting remote access for everyone behind it.

On the supply chain front, an attacker breached teamupdraft.com over the weekend of October 17-18, 2026, and took the vendor's customer database, including **UpdraftCentral** Cloud connection keys. Within hours, they used those keys to push backdoor plugins to WordPress sites through the UpdraftCentral channel built into UpdraftPlus, a backup plugin with over four million active installations. Together, these incidents underscore a growing trend of hybrid cyber operations that combine technical exploitation with social engineering, reinforcing the need for timely patching, continuous monitoring, and layered security defenses.



High Level Statistics

3
Attacks Executed

9
Vulnerabilities Exploited

1
Adversaries in Action

- Sirius Backdoor
- XMRig
- myawesomeproxy

- CVE-2026-109618
- CVE-2026-109619
- CVE-2026-111497
- CVE-2026-96652
- CVE-2026-96654
- CVE-2026-96655
- CVE-2026-96656
- CVE-2026-105482
- CVE-2026-76418

- Lazarus

Insights

Attackers broke into teamupdraft.com and stole the **UpdraftCentral** keys, so one vendor breach reached WordPress sites that were never attacked directly.

Plex2Shell chains **CVE-2026-96652**, **CVE-2026-96654**, **CVE-2026-96655**, and **CVE-2026-96656** into remote code execution, so update Plex Media Server now.

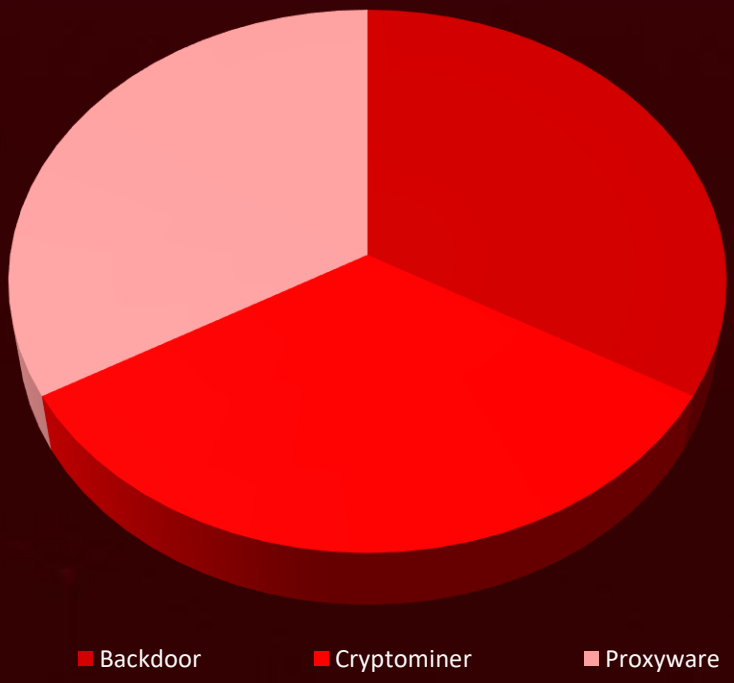
CVE-2026-105482 cuts a hostname short at a null byte, so an app can check one domain and look up a completely different one.

CVE-2026-76418 forces the firewall to reload, so remote staff, administrators, and partners can all be cut off at once.

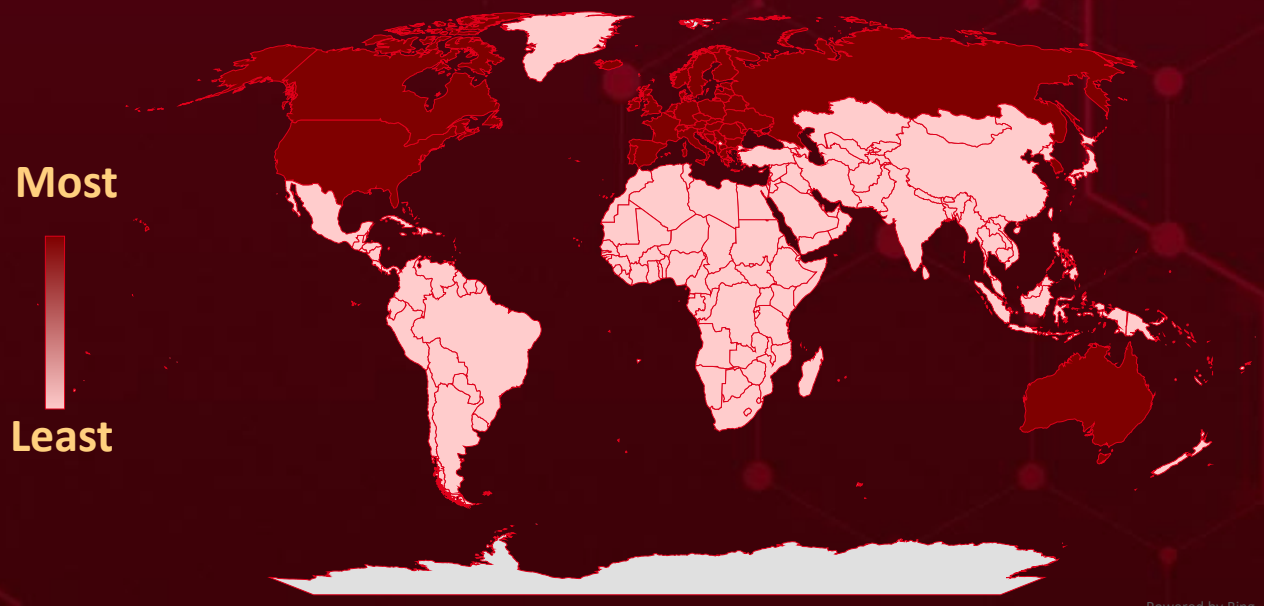
Debian, **Red Hat**, **OpenSUSE**, and **Ubuntu** were all affected, so it doesn't matter which Linux you run; you have updates waiting.

A fake **FedEx** tax invoice is delivering a new variant of the **Sirius** Backdoor, so think twice before opening any invoice you weren't expecting.

Threat Distribution



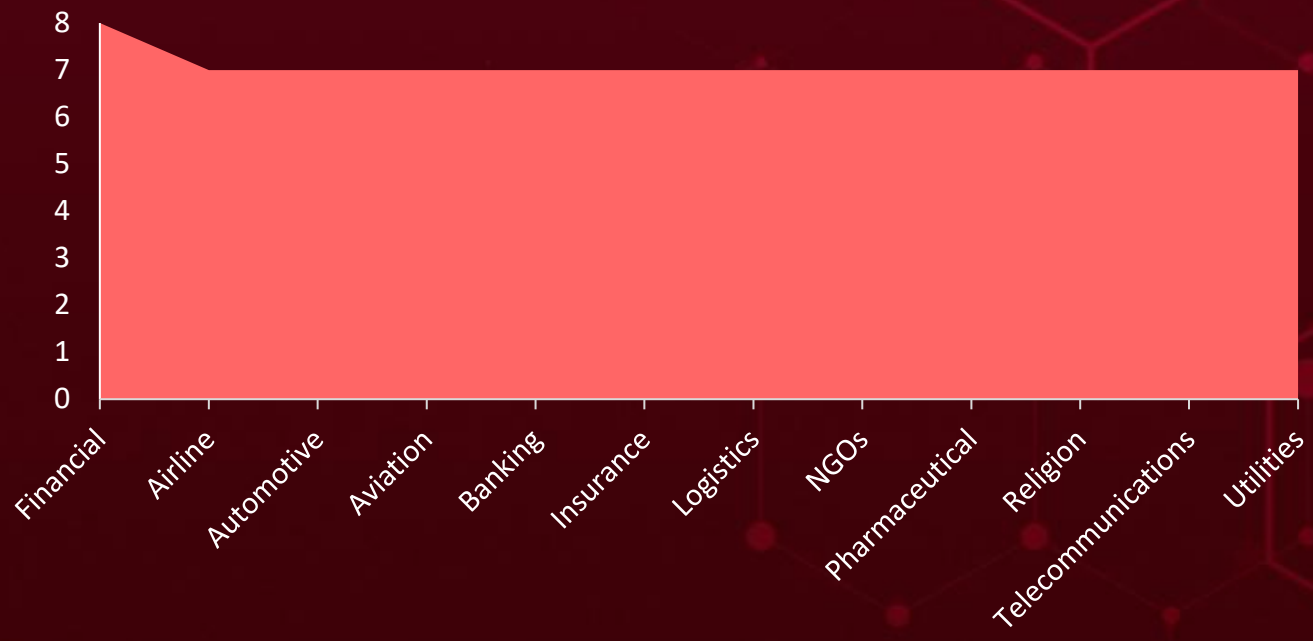
Targeted Countries



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

Countries	Countries	Countries	Countries
Norway	Czech Republic	Lithuania	Dominican Republic
United States	Moldova	Latvia	North Korea
Slovakia	Denmark	Argentina	Ecuador
Albania	Montenegro	New Zealand	Panama
Monaco	Estonia	Turkmenistan	Egypt
Andorra	North Macedonia	Armenia	Qatar
Romania	Finland	Philippines	El Salvador
Australia	Poland	Cuba	Saint Lucia
Sweden	France	Swaziland	Equatorial Guinea
Austria	Republic of Ireland	Curacao	Canada Quebec
Malta	Germany	Morocco	American Samoa
Belarus	Russia	Cyprus	Chad
Netherlands	Greece	Brunei	Ethiopia
Belgium	Serbia	Aruba	Taiwan
Portugal	Holy See	Rwanda	Faroe Islands
Bosnia and Herzegovina	Slovenia	Democratic Republic of Congo	Tonga
San Marino	Hungary	Cape Verde	Fiji
Bulgaria	Spain	Algeria	United Arab Emirates
South Korea	Iceland	Tibet	Azerbaijan
Canada	Switzerland	Djibouti	Vietnam
Ukraine	Italy	Uruguay	Bahamas
Croatia	United Kingdom	Dominica	
Luxembourg	Liechtenstein	Nauru	

Targeted Industries



TOP MITRE ATT&CK TTPs

T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1588** Obtain Capabilities	**T1071** Application Layer Protocol	**T1105** Ingress Tool Transfer
T1499 Endpoint Denial of Service	**T1210** Exploitation of Remote Services	**T1505.003** Web Shell	**T1203** Exploitation for Client Execution	**T1211** Exploitation for Defense Evasion
T1496 Resource Hijacking	**T1212** Exploitation for Credential Access	**T1550** Use Alternate Authenticatio n Material	**T1564** Hide Artifacts	**T1036** Masquerading
T1098 Account Manipulation	**T1505** Server Software Component	**T1041** Exfiltration Over C2 Channel	**T1005** Data from Local System	**T1053** Scheduled Task/Job

Attacks Executed

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**
-			-
IOC TYPE	**VALUE**		
SHA256	d6802fce5b918ed247ba85d6aa0545a8120cfbc3734b1c37794c4e381862d4ee		

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="5">XMRig is an open-source cryptocurrency miner that is widely abused to hijack the processing power of compromised systems. In this campaign it is deployed on Plex Media Server hosts compromised through Plex2Shell, causing sustained high CPU use.</td><td>Exploiting vulnerabilities</td><td>CVE-2026-96652
CVE-2026-96654
CVE-2026-96655
CVE-2026-96656</td></tr>
<tr><td>TYPE</td><td>IMPACT</td><td>AFFECTED PLATFORM</td></tr>
<tr><td>Cryptominer</td><td rowspan="3">Compute hijacking, degraded performance, higher power and hosting costs</td><td>Plex Media Server</td></tr>
<tr><td>ASSOCIATED ACTOR</td><td>PATCH LINK</td></tr>
<tr><td>-</td><td>https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319</td></tr>
<tr><td>IOC TYPE</td><td colspan="3">VALUE</td></tr>
<tr><td>SHA256</td><td colspan="3">2d3c618b21a7e2f8bcd735da188e44a7609ff3f204832dd0781cd09e4388c9db</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 CVE-2026-96654 CVE-2026-96655 CVE-2026-96656
TYPE		**IMPACT**	**AFFECTED PLATFORM**
Proxyware		Bandwidth hijacking, victim IP abused to relay traffic, harder attribution	Plex Media Server
ASSOCIATED ACTOR			**PATCH LINK**
-			https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319

IOC TYPE	VALUE
SHA256	e546b10aee5edc754da4f9b0baace00392257121911f630145078eafad1e6bd9

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-2026-109618	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 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 Stale Internal Request-State 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/ HTTP2Shell/ Broccoli2Shell	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), 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:node.js:*:*:*:*:*:*:*:* cpe:2.3:a:google:brotli:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:.net:*:*:*:*:*:*:*:*	-
Google Brotli Unchecked Return Value Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787 CWE-252	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1499: Endpoint Denial of Service	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/

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-96652	Plex2Shell 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 Server-Side Request Forgery (SSRF) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	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-2026-96654</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 Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability</td><td></td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINKS</td></tr>
<tr><td>CWE-84</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-2026-96655	Plex2Shell 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 Server-Side Request Forgery (SSRF) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-918	T1190: Exploit Public-Facing Application, T1550.001: Application Access Token, T1105: Ingress Tool Transfer	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-2026-96656</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>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2026-105482		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)	-
	ZERO-DAY		
		**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:nodejs:node.js:*:*:*:*:*:*:*:*	-
Node.js DNS Null Byte Truncation Vulnerability			
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-284	T1190: Exploit Public-Facing Application, T1071: Application Layer Protocol	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/

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

Adversaries in Action

NAME	ORIGIN	TARGETED INDUSTRIES	TARGETED REGIONS
 Lazarus	North Korea	Government, financial, logistics, airports, manufacturing, and online transaction platforms	USA, Japan, Thailand, Indonesia, South Korea, Australia, Taiwan, India, Singapore, UAE, Saudi Arabia, and the EU
	MOTIVE		
	Information theft and espionage, Sabotage and destruction, Financial crime		
	TARGETED CVE	**ASSOCIATED ATTACKS/RANSOM WARE**	**AFFECTED PRODUCT**
	CVE-2026-109618 CVE-2026-109619	-	PHP

TTPs
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

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **nine exploited vulnerabilities** and block the indicators related to the threat actor **Lazarus** and the malware **Sirius Backdoor, XMRig,** and **myawesomeproxy**

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 **nine exploited vulnerabilities.**
- Testing the efficacy of their security controls by simulating attacks related to the threat actor **Lazarus** and the malware **Sirius Backdoor** in Breach and Attack Simulation(BAS).

Threat Advisories

Stolen Keys, Trusted Channel: UpdraftCentral Backdoors WordPress at Scale

Sirius Backdoor Hides Behind Fake FedEx Invoices

Plex2Shell Exploit Chain Actively Exploited to Hijack Plex Media Servers

CVE-2026-105482: Node.js Trusts a Name It Never Looked Up

Cisco Firewall Zero-Day Lets Anyone Reboot Your VPN

October 2026 Linux Patch Roundup

PHP2Shell: Your Application Code Is Clean, But the Engine Underneath It Isn't

Node2Shell: Node.js Brotli Flaw Turns Compressed Data into Code Execution

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
Sirius Backdoor	SHA256	d6802fce5b918ed247ba85d6aa0545a8120cfbc3734b1c37794c4e381862d4ee
	MD5	e8b080c276519547e95930ab15028adb
XMRig	SHA256	2d3c618b21a7e2f8bcd735da188e44a7609ff3f204832dd0781cd09e4388c9db
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 02, 2026 • 8:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com