TransilienceAI

Plex2Shell exploit chain

Threat Report · TLP:CLEAR

campaign · Plex2Shell

21 Oct 2026

Version 4 · 6 sources

TLP:CLEAR — Transilience Newsroom

Compiled by Transilience from public reporting. May be shared without restriction.

Table of Contents

BRIEF . . . 3

- Bottom line . . . 3
- For the board . . . 3
- Are you exposed? . . . 3
- What to do . . . 3

TIMELINE . . . 4

WHAT THEY DID . . . 4

WHOM THEY TARGET . . . 4

MALWARE AND TOOLS . . . 4

ATTRIBUTION . . . 5

DISRUPTION, ADVISORIES AND LAW ENFORCEMENT . . . 5

ATT&CK; TECHNIQUES . . . 5

INDICATORS . . . 5

NOT KNOWN YET . . . 5

SOURCES . . . 5

ABOUT THIS REPORT . . . 6

Brief

ACTIVE
""As of this morning (Oct 17th), I finally saw in the wild exploitation," the researcher wrote." [1]

Bottom line

Public Plex2Shell exploit and PoC were weaponized within a day to install XMRig miners and a residential proxy on unpatched, internet-facing Plex servers; observed so far against a honeypot. If you expose Plex, update immediately, and hunt for miner/proxy indicators and unknown outbound connections. [1,2,3]

For the board

A public exploit for chained Plex vulnerabilities is being actively used to install cryptominers and proxy software on internet-exposed, unpatched Plex servers; patch and isolate exposed instances now.

Are you exposed?

Targets	How to check
Internet-facing Plex Media Server instances (pre-1.43.3.10861). [3,4]	Is Plex exposed publicly or running versions before 1.43.3.10861; look for high CPU, unknown child processes, unfamiliar codecs.

What to do

1. **Patch Plex Media Server to 1.43.3.10861 or later immediately.** [1,3]
   Plex released fixes in September that address the four chained vulnerabilities enabling unauthenticated RCE; attackers weaponized the PoC.
2. **Hunt for XMRig processes, 'mylovelyminer', and 'myawesomeproxy' artifacts and outbound connections.** [1,2]
   Observed payloads include an XMRig miner and a proxy backdoor that create CPU spikes and outbound proxy traffic.
3. **Block or monitor inbound access to Plex from the internet until patched.** [1,4]
   Exploit chain targets internet-facing Plex; early attacks were against an internet-facing honeypot.
4. **Investigate unfamiliar files in Plex Codecs directory and unexpected child processes.** [3]
   The chain writes a malicious .so in the Codecs directory which runs under the Plex service account.

Also reported as cryptominer · myawesomeproxy · residential proxy software.

Timeline

Date	Kind	What happened
July 27, 2026	DISCLOSURE	Vulnerabilities reported to Plex. [1] *“The issues were reported to Plex on July 27, and the company confirmed them and awarded a bug bounty on August 4.”* [1]
October 16, 2026	DISCLOSURE	Researcher published Plex2Shell write-up and PoC. [1] *“The researcher who found the Plex2Shell bugs released a write-up and proof-of-concept (PoC) code on October 16.”* [1]
October 17, 2026	EXPLOITATION	In-the-wild exploitation observed against vulnerable Plex honeypot. [1] *““As of this morning (Oct 17th), I finally saw in the wild exploitation,” the researcher wrote.”* [1]
October 17, 2026	CAMPAIGN	Attackers deployed XMRig miner and 'myawesomeproxy' on honeypot. [1] *“The attackers were observed dropping a cryptocurrency miner built on XMRig. Later that day, a second program called myawesomeproxy also appeared on the honeypot.”* [1]
2026-10-21 published	ADVISORY	CISA added Plex2Shell to KEV and set patch deadlines. [5] *“CISA... added four vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog, including four vulnerabilities impacting Plex Media Server that's collectively called Plex2Shell.”* [5]

What they did

Count	Detail
observed against a honeypot	Exploit attempts and successful honeypot infections deploying XMRig and myawesomeproxy. [1] *“The attackers were observed dropping a cryptocurrency miner built on XMRig. Later that day, a second program called myawesomeproxy also appeared on the honeypot.”* [1]

Whom they target

- Residential IPs used as proxy nodes [1]
  “Plex may be hosted on residential IP and I think threat actors would love to have residential IP proxy to access corporate VPNs and emails,” [1]

Malware and tools

Count	Detail
1 miner family	XMRig-based miner (identified as 'mylovelyminer' or XMRig) [2] *“Also deployed concurrently is an XMRig miner process identified as "mylovelyminer" with its mining server pointing to "ota.proxystream[.]st.”"* [2]

1 proxy artifact	'myawesomeproxy' residential proxy/backdoor [2] *“Furthermore, the vulnerabilities have been exploited to deliver an artifact named "myawesomeproxy," which, according to VirusTotal, is a stealthy Linux backdoor and reverse proxy.”* [2]
1 PoC	Exploit PoC code for the Plex2Shell vulnerability chain [1] *“The researcher who found the Plex2Shell bugs released a write-up and proof-of-concept (PoC) code on October 16.”* [1]

Attribution

- Unknown criminal actors; opportunistic weaponization of public PoC. [1]
  “The attackers used the publicly released exploit, the researcher said, though they may have tweaked the code.” [1]

Disruption, advisories and law enforcement

None reported.

ATT&CK techniques

ID	Technique	Mapped from
T1105	**Ingress Tool Transfer** MAPPED BY NEWSROOM	*“The attacks led to the deployment of a miner payload from a remote server ("217.60.194[.]116").”* [2]

Indicators

Kind	Indicator
DOMAIN	`proxystream[.]st` [2]

Not known yet

- Scope beyond honeypot observations
- Number of compromised real-world servers
- Whether observed residential IPs were abused to access corporate resources

Sources

#	Outlet	Article	Copy
1	**SecurityWeek** 19 Oct 2026	Plex2Shell Exploit Chain Weaponized Against Plex Servers Hours After Disclosure	archived copy

2	**The Hacker News** 19 Oct 2026	Hackers Exploit Plex2Shell Flaws to Install Crypto Miners and Linux Proxy Backdoor	archived copy
3	**Security Affairs** 19 Oct 2026	Plex2Shell Exploit Used to Turn Vulnerable Plex Servers Into Crypto Miners - Security Affairs	archived copy
4	**Ars Technica — Security** 19 Oct 2026	Recently fixed Plex Media vulnerabilities are being exploited to install malware	archived copy
5	**The Hacker News** 21 Oct 2026	CISA Orders Federal Agencies to Patch Exploited Plex2Shell, Siemens, and SiteGuard Flaws	archived copy
6	**BleepingComputer (Bluesky)** 21 Oct 2026	CISA: Hackers chain Plex flaws in Plex2Shell attacks to breach servers	archived copy

About this report

Compiled by Transilience Newsroom from 6 public sources. Every quotation is checked against the article it cites; 7 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked “mapped by Newsroom” are our reading of the quoted behaviour, not the source's claim. Version 4, written 21 October 2026, 18:54 UTC (threat-report-2026-09-25b). TLP:CLEAR — may be shared without restriction. The live report: https://threatnews.transilience.cloud/report/threat/mvf9bya7g1lt