Hive Pro

Threat Level

Red

Hiveforce Labs

# THREAT ADVISORY

## VULNERABILITY REPORT

# Plex2Shell Exploit Chain Actively Exploited to Hijack Plex Media Servers


| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| October 29, 2026 | A1 | TA2026318 |

# Summary

**First Seen:** July 27, 2026
**Malware:** XMRig, myawesomeproxy
**Affected Products:** Plex Media Server
**Impact:** Plex2Shell is an exploit chain that combines four Plex Media Server vulnerabilities, CVE-2026-96652, CVE-2026-96654, CVE-2026-96655, and CVE-2026-96656. It lets an unauthenticated remote attacker reach internal functions, recover the server owner's administrator token, and plant a malicious library in the Codecs directory to run code. Fixes shipped in version 1.43.3.10861 in August 2026, but a public proof of concept released on October 16, 2026 was weaponized within a day. Unpatched internet-facing servers are now being widely exploited to deploy XMRig cryptocurrency miners and myawesomeproxy proxyware, which turns victim systems into monetized relay nodes with a foothold in their surrounding networks.

## CVEs

| CVE | NAME | AFFECTED PRODUCT | ZERO-DAY | CISA KEV | PATCH |
|---|---|---|---|---|---|
| CVE-2026-96652 | Plex2Shell (Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability) | Plex Media Server | ✗ | ✓ | ✓ |
| CVE-2026-96654 | Plex2Shell (Plex Media Server Improper Neutralization of Encoded URI Schemes in a Web Page Vulnerability) | Plex Media Server | ✗ | ✓ | ✓ |
| CVE-2026-96655 | Plex2Shell (Plex Media Server Server-Side Request Forgery (SSRF) Vulnerability) | Plex Media Server | ✗ | ✓ | ✓ |
| CVE-2026-96656 | Plex2Shell (Plex Media Server External Control of File Name or Path Vulnerability) | Plex Media Server | ✗ | ✓ | ✓ |

# Vulnerability Details

**#1**

Plex Media Server is a self-hosted media streaming platform that listens on TCP port 32400 and is routinely exposed to the internet through its Remote Access feature or manual port forwarding. The server exposes multiple web-facing APIs, issues requests to internal services, and loads codec libraries for media processing, and the Plex2Shell chain abuses each of these legitimate functions to move from unauthenticated access to code execution. All versions earlier than 1.43.3.10861 are affected.

**#2**

CVE-2026-96652 is an unauthenticated server-side request forgery (CWE-918) in the player timeline endpoint that lets a remote attacker make the server issue requests to destinations of the attacker's choosing. CVE-2026-96654 stems from improper neutralization of URL values in the searchOne parameter, allowing an attacker to invoke other plugins' functions with attacker-supplied parameters and reach internal agent functions over the loopback interface.

**#3**

CVE-2026-96655 is a second server-side request forgery in the universal transcode endpoint that lets an authenticated requester reach arbitrary internal or external addresses, which the chain abuses with the stolen owner token to fetch attacker-controlled media, while CVE-2026-96656 permits an arbitrary file write to the Codecs directory through transcoder preferences. Individually the flaws score CVSS 5.3 for CVE-2026-96652 and CVE-2026-96655, 6.9 for CVE-2026-96654, and 8.6 for CVE-2026-96656, but the complete chain is rated CVSS 9.8.

**#4**

An attacker first abuses the request forgery and loopback weaknesses to reach privileged internal functions and recover the owner's administrator token. The chain then forces the server to retrieve attacker-controlled content and abuses transcoder preferences to plant a malicious shared library in the Codecs directory, after which code executes without valid credentials or user interaction. Exploitation requires network access to TCP port 32400, so servers reachable only internally remain exploitable from the same network, and the public proof of concept also needs the server to connect outbound to attacker infrastructure to fetch a carrier video and return a reverse shell.

**#5**

Fixes shipped in early August 2026, yet a public write-up and proof of concept released on October 16, 2026 were weaponized within a day, and Plex confirms active, widespread exploitation of unpatched internet-facing servers. Compromised hosts have been used to run XMRig miners and the myawesomeproxy reverse-proxy tool, while code execution under the service account exposes mounted shares, stored credentials, and adjacent internal services. Dropped libraries and modified transcoder settings can survive the upgrade, leaving previously exploited servers compromised after patching.

# Vulnerabilities

| CVE ID | AFFECTED PRODUCTS | AFFECTED CPE | CWE ID |
|---|---|---|---|
| CVE-2026-96652 | Plex Media Server (Before 1.43.3.10861) | cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:* | CWE-918 |
| CVE-2026-96654 | Plex Media Server (Before 1.43.3.10861) | cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:* | CWE-84 |
| CVE-2026-96655 | Plex Media Server (Before 1.43.3.10861) | cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:* | CWE-918 |
| CVE-2026-96656 | Plex Media Server (Before 1.43.3.10861) | cpe:2.3:a:plex:media_server:*:*:*:*:*:*:*:* | CWE-73 |

# Recommendations

**Upgrade Plex Media Server Immediately:** Update every Plex Media Server instance to version 1.43.3.10861 or later, which is not affected by any of the four vulnerabilities in the chain. Confirm the running build in Plex Web under Settings → General rather than trusting the update channel, because NAS package managers may lag behind the vendor release and those deployments may need the package installed manually from the Plex downloads page. Do not treat “1.43.3” alone as safe, because early 1.43.3 builds such as 1.43.3.10828 remain vulnerable, so verify that the full build number is 1.43.3.10861 or later.

**Treat Exposed Unpatched Servers as Compromised:** Assume compromise on any server that ran a version older than 1.43.3.10861 while reachable from the internet until proven otherwise. Hunt for processes spawned by Plex Media Server that are not recognized, particularly myawesomeproxy, mylovelyminer, or x12345, unfamiliar .so or .dll files in the Plex Codecs folder, transcoder options in Preferences.xml that no administrator set, outbound connections to proxystream[.]st, and sustained high CPU utilization while nothing is playing.

**Rebuild Compromised Servers and Reset Credentials:** Where compromise is confirmed or cannot be ruled out, rebuild the server from a clean installation instead of reusing the old Plex data directory, and at minimum purge the entire Codecs folder and review Preferences.xml. Sign out of all devices from the Plex account settings, change the Plex password to invalidate any exposed administrator token, and treat every mounted share and credential reachable by the Plex service account as potentially exposed.

**Reduce Internet Exposure:** Disable Remote Access under Settings → Remote Access wherever it is not required, and avoid forwarding TCP port 32400 directly to the internet. Where remote streaming is a business need, place the server behind a VPN or an authenticated reverse proxy so the vulnerable APIs are not reachable by unauthenticated parties.

**Restrict Outbound Traffic from Media Servers:** The public proof of concept depends on the server connecting outbound to attacker infrastructure, and post-exploitation proxyware relies on unrestricted egress. Limit outbound connections from media hosts to required Plex services, block proxystream[.]st at DNS and perimeter controls, and alert on new or high-volume outbound sessions originating from the Plex process.

**Enforce Least Privilege and Segmentation:** Run Plex Media Server under a dedicated low-privilege service account with read-only access to media libraries, and keep it off network segments that host backups, management interfaces, or sensitive file shares, so that code execution in the Plex process does not translate into broader network access.

# Potential MITRE ATT&CK TTPs

| Tactic | Technique | Sub-technique |
|---|---|---|
| Initial Access | T1190: Exploit Public-Facing Application | |
| Execution | T1129: Shared Modules | |
| | T1059: Command and Scripting Interpreter | T1059.004: Unix Shell |
| Persistence | T1574: Hijack Execution Flow | |
| Defense Evasion | T1550: Use Alternate Authentication Material | T1550.001: Application Access Token |
| Credential Access | T1212: Exploitation for Credential Access | |
| Command and Control | T1105: Ingress Tool Transfer | |
| Impact | T1496: Resource Hijacking | T1496.001: Compute Hijacking |
| | | T1496.002: Bandwidth Hijacking |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| Domains | ota[.]proxystream[.]st, global[.]relay[.]proxystream[.]st |
| SHA256 | 5712ef510481f15fe8b18fdd10b73026d57cb3d9d151878a692358b99a464441, 68938fb428f2bcfef4ede62f7b29cd0f15f37ed59e94462c099f2ca64e36baa7, b20f39fc00d242e706b6c30367ad811c676e0575050a4ec2f30104b696944b49, e546b10aee5edc754da4f9b0baace00392257121911f630145078eafad1e6bd9, 2d3c618b21a7e2f8bcd735da188e44a7609ff3f204832dd0781cd09e4388c9db |
| IPv4 | 45[.]194[.]92[.]222, 91[.]92[.]40[.]202, 176[.]65[.]139[.]228, 217[.]60[.]194[.]116 |

## 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/

## References

https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319

https://fieldeffect.com/blog/active-exploitation-plex2shell-vulnerabilities

https://www.boredhackerblog.info/2026/10/plex-vulnerabilities-being-exploited-in.html

https://github.com/code-zm/plex2shell

# 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 29, 2026 • 05:45 AM**

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com