GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

21 October 2026

Advisory 363: Plex Media Server Unauthenticated Remote Code Execution Chain (Plex2Shell) - Actively Exploited (CVE-2026-96652, CVE-2026-96654, CVE-2026-96655 and CVE-2026-96656).

Release Date: 20th October 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

Four vulnerabilities in Plex Media Server, publicly known as Plex2Shell, can be chained so that an unauthenticated remote attacker runs code on the server as the account running Plex. CERTVU has combined them in one advisory because they share the same product, the same fixed build and a single attack chain.

The four flaws are: CVE-2026-96652, an unauthenticated server-side request forgery (SSRF) through the /player/timeline endpoint, where the protocol parameter is put into a player URL without validation; CVE-2026-96654, improper handling of URLs in the searchOne endpoint (CWE-84), which lets the attacker call other plugins' functions and obtain the owner's admin token; CVE-2026-96655, an SSRF by an authenticated user through the /video/:/transcode/universal path (CWE-918); and CVE-2026-96656, external control of a file name or path (CWE-73), where the x264 transcoder option setting lets an administrator write a shared object (.so) file into the Plex Codecs directory, which Plex then loads without signature, execute-bit or symbol checks. In the reported chain, the SSRF forces a request to an internal agent over loopback, the owner's admin token is attached, the attacker sets transcoder options, and transcoding a crafted video drops and loads the shared object.

What are the systems affected?

The following product is affected:

- Plex Media Server before version 1.43.3.10861, on all platforms including Windows, macOS, Linux, NAS packages and container images
- Early 1.43.3 builds such as 1.43.3.10828 are still vulnerable, and may be mistaken for patched. Censys counts nearly 8,000 servers on that build

Not affected / patched version:

- Plex Media Server 1.43.3.10861 or later
- Windows and macOS installations may update automatically if enabled. Linux, NAS and Docker installations need a manual update

What does this mean?

Successful exploitation may allow attackers to:

- Run arbitrary code on the media server as the account running Plex, without logging in
- Install cryptocurrency miners and proxy backdoors, using the server and the owner's internet connection for abuse
- Reach mounted shares and any credentials available to the Plex service account, and use the server as a foothold in the home or office network

Mitigation process

CERTVU recommends the following:

1. Update Plex Media Server
Update every installation to 1.43.3.10861 or later, and confirm the running build because 1.43.3.10828 is still vulnerable. Update manually on Linux, NAS and Docker. Do not expose Plex directly to the internet where remote access is not needed.

2. Treat older internet-facing servers as possibly compromised
Updating does not remove an implant already in the Codecs folder or revoke an exposed admin token. For any server that ran an older build while internet-reachable, clear the Codecs directory, check Preferences.xml for unexpected transcoder options (TranscoderH264Options), and consider a clean reinstall.

3. Hunt for indicators

4. Reset access

Report suspected compromise to CERTVU.

Reference

1. https://censys.com/advisory/cve-2026-96652-cve-2026-96654-cve-2026-96655-cve-2026-96656/
2. https://thehackernews.com/2026/10/hackers-exploit-plex2shell-flaws-to.html
3. https://www.sentinelone.com/vulnerability-database/cve-2026-96656/

4. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
5. https://nvd.nist.gov/vuln/detail/CVE-2026-96656