contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Plex Media Server exploited

CVE-2026-96656 · on CISA's exploited list since 20 October 2026

Analysis Report

Anyone running Plex Media Server older than 1.43.3.10861 should update now, because CISA's 23 October 2026 date has passed. If that server is reachable from the internet, treat it as possibly …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 4.0 8.6**	STATUS	On CISA's exploited list; due 23 October 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/plex-media-server-cve-2026-96656

The bottom line

> *Anyone running Plex Media Server older than 1.43.3.10861 should update now, because CISA's 23 October 2026 date has passed. If that server is reachable from the internet, treat it as possibly compromised and check it before relying on the update. If you do not run Plex, stop here.*

At a glance

Fact	Detail
Product	Plex Media Server (CVE-2026-96656)
Severity	High: 8.6 (CVSS 4.0)
CISA	On its exploited list since 20 October 2026. Deadline for US federal agencies: 23 October 2026.
Chance of exploitation (EPSS)	0.02, the estimated chance in the next 30 days, as at 1 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Plex Media Server 1.43.3.10861 and later are not affected (vendor's post of 19 October 2026 and the record).
Who looks first	Anyone who runs Plex Media Server below 1.43.3.10861, above all on a NAS, home server or VM that is reachable from the internet, or that shares a machine with credentials or mounted shares.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Plex Media Server on any machine, NAS or VM?	Nothing to do for this CVE.	Check the version (next question).
Is the version older than 1.43.3.10861?	The record lists you as unaffected. Still check for signs of compromise if you were exposed earlier.	Update now and treat the server as possibly compromised.
Is the server reachable from the internet, for example by forwarding port 32400?	Exposure is lower, but still update. The chain needs the server to be reachable.	Highest priority: reduce exposure, update, then check for compromise.

Do you see unknown processes, unknown .so or .dll files in Codecs, or high CPU while nothing plays?	Keep the update and the exposure changes.	Rebuild from a clean install and rotate credentials.

What it is

An admin user can set a transcoder preference that is appended unchecked to the encoder's options on every transcode. That writes files of their choosing. The server loads every .so file at startup without checks, so a planted file runs. Chained with three other flaws, no login is needed.

Why it matters

Our reading: on its own this flaw needs an admin account, which is why its score is lower than the exploitation suggests. The vendor says it was chained with CVE-2026-96652, CVE-2026-96654 and CVE-2026-96655 to give an unauthenticated remote attacker code execution as the Plex process. The vendor reports compromised servers running cryptocurrency miners and proxy software that routes other people's traffic through the victim's connection. Anything the Plex service account can reach is then exposed.

What the vendor's advisory says

We read three pages on forums.plex.tv and raw.githubusercontent.com. In short:

- The vendor's post says the fixes are in Plex Media Server 1.43.3.10861, and that the same release fixes CVE-2026-96652, CVE-2026-96654 and CVE-2026-96655.
- The vendor describes CVE-2026-96652 as unauthenticated server-side request forgery in the player timeline endpoint.
- The vendor describes CVE-2026-96654 as access to internal agent functions over the loopback interface, and CVE-2026-96655 as disclosure of the server owner's admin token.
- The vendor says a public proof of concept was released on 16 October 2026 and attacks on internet-facing, un-updated servers have been widespread since.
- The CSAF record scores this CVE 7.2 (CVSS 3.1, high privileges required); CVE-2026-96655 is scored 4.3. The record for this CVE says 8.6 under CVSS 4.0.

Things people will get wrong

- It needs an admin, so it is a low risk The vendor says it was chained with three other flaws to give an unauthenticated remote attacker code execution. One of them discloses the admin token.
- I updated, so I am clean The vendor says an older, internet-facing server may already be compromised. Updating does not remove planted files or processes.

- Only media files are at risk The vendor says to treat anything the Plex service account can reach, such as mounted shares and stored credentials, as potentially exposed.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the versions you run

- In Plex Web, open Settings, then General, and read the version shown.
- Anything older than 1.43.3.10861 is affected, according to the record.

```
dpkg -l plexmediaserver
```

Step 2: Reduce exposure

- If you do not need remote access, turn it off under Settings, then Remote Access, as the vendor advises.
- Avoid forwarding port 32400 directly unless you need it.

Step 3: Update and check for compromise

- Update to 1.43.3.10861 or newer, using the vendor's update instructions for your platform.
- Look for unknown processes, unfamiliar .so or .dll files in Codecs, and transcoder options you did not set in Preferences.xml.

Step 4: If you find anything, rebuild

- Rebuild from a clean install instead of reusing the old data directory. At minimum, empty Codecs and review Preferences.xml.
- Sign out all devices, change the Plex password, and treat reachable shares and stored credentials as exposed.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to confirm our exposure to CVE-2026-96656 in Plex Media Server, which CISA lists as exploited. Please tell us whether we run Plex Media Server anywhere, on which machines, and which version. The fixed version is 1.43.3.10861; anything older is affected. Please also say whether port 32400 is reachable from the internet. Please update any affected server, check the Codecs folder and Preferences.xml for anything unexpected, and confirm the version and the result of those checks in writing by the date you give us. Thank you.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Processes started by Plex that you do not recognise, such as names like myawesomeproxy, mylovelyminer or x12345, according to the vendor.
- Unfamiliar .so or .dll files in the Plex Codecs folder, and transcoder options in Preferences.xml that you did not set.
- Sustained high CPU use while nothing is playing, or unexpected outbound connections from the Plex machine.

The weakness behind it

The record classes this as CWE-73 (External Control of File Name or Path).

The sources, in their words

CISA's catalogue entry:

> *Plex Media Server contains an external control of file name or path vulnerability which can allow an admin user to write arbitrary files that may be executed on load. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96654, and CVE-2026-96655.*

The CVE record, published by Cisa-cg on 23 September 2026:

> *Plex Media Server before 1.43.3.10861 allows an admin user to write arbitrary files that may be executed on load. The preference TranscoderH264Options is appended verbatim to x264's option string on every transcode. At startup, all .so files are run without signature, execute bit, or symbol checks.*

Versions of Plex Media Server the record lists as affected:

- all versions before 1.43.3.10861

It lists these as unaffected:

- 1.43.3.10861

The affected ranges end before 1.43.3.10861. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

What we do not know yet

- The sources do not say how many servers were compromised or whether the exploitation was targeted.
- The sources do not say whether the Codecs folder and Preferences.xml checks catch every kind of compromise.
- The sources do not say whether older releases get a separate fix; they name only 1.43.3.10861.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-96656: score 8.6, `CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Attack requirements	None	Works against a default deployment.
Privileges required	High	An administrator account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	High	Total loss of confidentiality.
Vulnerable system: integrity	High	Total loss of integrity.
Vulnerable system: availability	High	Total loss of availability.
Subsequent systems: confidentiality	None	No data exposed.
Subsequent systems: integrity	None	Nothing can be altered.
Subsequent systems: availability	None	No effect on availability.

Appendix 2. Timeline

Date	Event
23 September 2026	CVE record published by Cisa-cg.
20 October 2026	CISA added it to its list of exploited vulnerabilities.
23 October 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe

Version below 1.43.3.10861 and reachable from the internet	High	Now; the CISA date has passed
Version below 1.43.3.10861 and signs of compromise found	High	Now: rebuild and rotate credentials
Version below 1.43.3.10861, reachable only on the local network	Medium	This week
Already on 1.43.3.10861 or later, previously exposed on an older version	Medium	This week: check for compromise
Not running Plex Media Server	None	None for this CVE

Appendix 4. Definition of done

- Every Plex Media Server you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-96656: https://www.cve.org/CVERecord?id=CVE-2026-96656
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: forums.plex.tv/t/important-security-update-for-plex-media-serv: https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319
- Advisory or release notes read: forums.plex.tv/t/plex-media-server/30447/711: https://forums.plex.tv/t/plex-media-server/30447/711
- Advisory or release notes read: raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/v: https://raw.githubusercontent.com/cisagov/CSAF/develop/csaf_files/IT/white/2026/va-26-266-01.json
- Reference in the CVE record: www.cve.org: https://www.cve.org/CVERecord?id=CVE-2026-96656
- Reference in the CVE record: zmain.info: https://zmain.info/blog/plex2shell