contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Plex Media Server exploited

CVE-2026-96655 · on CISA's exploited list since 20 October 2026

Analysis Report

If you run Plex Media Server, update it to 1.43.3.10861 or later by 3 November 2026. If you do not run it, you can stop reading. Start by finding which version each server is on.

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 4.0 5.3**	STATUS	On CISA's exploited list; due 3 November 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-2026-96655

The bottom line

> *If you run Plex Media Server, update it to 1.43.3.10861 or later by 3 November 2026. If you do not run it, you can stop reading. Start by finding which version each server is on.*

At a glance

Fact	Detail
Product	Plex Media Server (CVE-2026-96655)
Severity	Medium: 5.3 (CVSS 4.0)
CISA	On its exploited list since 20 October 2026. Deadline for US federal agencies: 3 November 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	1.43.3.10861 and later (the CVE record and the Plex forum post of 19 October 2026).
Who looks first	Anyone running Plex Media Server older than 1.43.3.10861. Look first at servers reachable from the internet, and at servers where people other than the owner hold accounts.

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 server older than 1.43.3.10861?	You are on a fixed version. Confirm it in writing.	Update it, then answer the next question.
Is the server reachable from the internet, for example by forwarding port 32400?	Lower urgency, but still update within CISA's window.	Treat it as urgent. Update now and check for signs of compromise.
Do people you do not fully trust hold accounts on the server?	The login requirement limits who can use this flaw directly.	Any of them could use it. Update before anything else.

What it is

An attacker with a login on the server can make it send requests to internal or external addresses of their choosing, through the transcode path. The record does not say what the attacker gets back. CISA says this flaw can be chained with three other Plex flaws.

Why it matters

Our reading is that this flaw is a stepping stone rather than the whole attack. It needs a login and its score is moderate. But CISA says it can be chained with CVE-2026-96652, CVE-2026-96654 and CVE-2026-96656. Plex says the chain lets an unauthenticated remote attacker run code as the Plex process. A request-forwarding flaw is useful for reaching addresses that the server can see and the attacker cannot.

What the vendor's advisory says

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

- The Plex forum post of 19 October 2026 lists four flaws fixed in 1.43.3: CVE-2026-96652, CVE-2026-96654, CVE-2026-96655 and CVE-2026-96656.
- Plex says the four, chained together, let an unauthenticated remote attacker run code with the privileges of the Plex Media Server process.
- Plex says they are being actively and widely exploited, and that a public proof of concept was released on 16 October.
- Plex says compromised servers have run cryptocurrency miners and proxy software that routes other people's traffic through the victim's connection.
- Plex says that if a server is older than 1.43.3.10861 and reachable from the internet, you should assume it may be compromised.

Things people will get wrong

- "It needs a login, so it is not urgent." CISA says it chains with other Plex flaws. Plex says the chain needs no login and lets an attacker run code on the server.
- "The score is only moderate, so it can wait." Plex says the flaws are actively and widely exploited. The score does not capture what the chain allows.
- "It is on our internal network, so we are safe." Plex's warning is aimed at internet-facing servers. A server shared with other users is still worth updating.

The wording includes conditions the score may not show: the attacker must be logged in. Read the record before you decide it does not apply to you.

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

- List every machine, NAS or VM that runs Plex Media Server. Include old ones that nobody uses.
- In Plex Web, open Settings, then General, and read the version shown. Compare it with 1.43.3.10861.

```
dpkg -l plexmediaserver
systemctl status plexmediaserver
```

Step 2: Reduce exposure

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

```
ss -tlnp | grep 32400
```

Step 3: Update to 1.43.3.10861 or later

- Follow Plex's update instructions for your platform. Some app stores may be slower to offer the update.
- Check the version again afterwards.

Step 4: Check for signs of compromise

- If the server was older than the fixed version and reachable from the internet, look for the signs listed below.
- If you cannot rule out compromise, Plex advises a rebuild from a clean install, signing out all devices and changing the Plex password.

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-2026-96655 in Plex Media Server, a flaw that lets a logged-in user make the server send requests to addresses of their choosing. Please tell us whether we run Plex Media Server anywhere, on which machines, and which version each is on. The fixed version is 1.43.3.10861. CISA has set a deadline of 3 November 2026. Plex also says related flaws are being actively exploited. Please update anything older, turn off remote access if we do not need it, and confirm in writing the version and the fix by 3 November 2026. 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, which Plex says include names like myawesomeproxy, mylovelyminer or x12345.
- Unfamiliar .so or .dll files in the Plex Codecs folder, or transcoder options in Preferences.xml that you did not set.
- Sustained high CPU use while nothing is playing, or unexplained outbound connections from the Plex machine.

The weakness behind it

The record classes this as CWE-918 (Server-Side Request Forgery).

The sources, in their words

CISA's catalogue entry:

> *Plex Media Server contains a server-side request forgery (SSRF) vulnerability that could allow an authenticated user to request arbitrary internal or external addresses via the '/video/:/transcode/universal' path parameter. This vulnerability can be chained with CVE-2026-96652, CVE-2026-96654, and CVE-2026-96656.*

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

> *Plex Media Server before 1.43.3.10861 allows an authenticated user to request arbitrary internal or external addresses via the '/video/:/transcode/universal' path parameter.*

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 record does not say what a successful request returns to the attacker, or whether internal services can be read.
- The Plex forum post describes CVE-2026-96655 as disclosure of the admin token, but the CVE record describes a request-forwarding flaw. The sources do not explain the difference.
- The sources do not say which accounts count as authenticated, for example whether a shared or invited user is enough.
- 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-2026-96655: score 5.3, `CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/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	Low	An ordinary account is enough.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	Low	Some data exposed.
Vulnerable system: integrity	None	Nothing can be altered.
Vulnerable system: availability	None	No effect on 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.
3 November 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

A server older than 1.43.3.10861 that faces the internet	High	Now, within CISA's window
An older server on a home or office network only, with several user accounts	Medium	This week, within CISA's window
An older server on a private network with one trusted account	Low	Next patch cycle, but before CISA's date
A server already on 1.43.3.10861 or later	Low	Confirm the version; nothing more for this CVE
You do not run 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-2026-96655: https://www.cve.org/CVERecord?id=CVE-2026-96655
- 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-2026-96655
- Reference in the CVE record: zmain.info: https://zmain.info/blog/plex2shell