contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Plex Media Server exploited

CVE-2026-96652 · on CISA's exploited list since 20 October 2026

Analysis Report

Anyone running Plex Media Server older than 1.43.3.10861 should update by 3 November 2026, and today if it faces the internet. Check the version in Settings → General first. If you run no Plex ...

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-2026-96652

The bottom line

> *Anyone running Plex Media Server older than 1.43.3.10861 should update by 3 November 2026, and today if it faces the internet. Check the version in Settings → General first. If you run no Plex server, you can stop reading.*

At a glance

Fact	Detail
Product	Plex Media Server (CVE-2026-96652)
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	Plex Media Server 1.43.3.10861 and later (the vendor's forum post of 19 October 2026 and the CSAF advisory file both name it)
Who looks first	Anyone running Plex Media Server before 1.43.3.10861, most of all a server reachable from the internet. That includes a home or office server with 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 anywhere, including a NAS or a spare PC?	Nothing to do for this CVE.	Check the version (next question).
Is the version older than 1.43.3.10861?	Fixed. Only check for compromise if it was older and exposed earlier.	Affected. Go to the next question.
Can the server be reached from the internet, for example by a port forward or remote access?	Lower risk, but still update. The vendor's warning is about internet-facing servers.	Update now, then check for signs of compromise.

What it is

An attacker with no account can make the Plex server send a request to any address they choose. The record says any X-Plex-Token value is accepted, and the attacker puts a full web address in the 'protocol' parameter of the '/player/timeline' endpoint.

Why it matters

The record says this flaw lets an attacker make the server send requests for them. The vendor's forum post of 19 October 2026 says it was chained with CVE-2026-96654, CVE-2026-96655 and CVE-2026-96656 to run code as the Plex process. It also says compromised servers ran cryptocurrency miners and proxy software. Our reading is that the 4.3 score in the CISA advisory file understates it: this is one link in an attack chain. Treat the four flaws as one problem.

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 Plex Media Server 1.43.3.10861 and later are not affected by the four chained flaws.
- It also lists CVE-2026-96654 (internal agent functions over the loopback interface), CVE-2026-96655 (disclosure of the admin token) and CVE-2026-96656 (arbitrary file write to the Codecs directory).
- The vendor says a public proof of concept was released on 16 October, followed by widespread attacks on internet-facing servers that were not updated.
- The vendor says that if your server is older than 1.43.3.10861 and reachable from the internet, you should assume it may be compromised.
- If you find signs of compromise, the vendor says to rebuild from a clean installation, sign out of all devices and change your Plex password.

Things people will get wrong

- "It only scores 4.3, so it can wait." The vendor says it is part of a chain that gives remote code execution, and that it is being actively exploited.
- "It needs a token, so the attacker needs an account." The record says any X-Plex-Token value works. The vendor calls the flaw unauthenticated.
- "Updating cleans up a server that was already hit." The vendor says a compromised server should be rebuilt from a clean installation, not reuse the old data directory.

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 Plex Media Server, including those on a NAS, in Docker or on a spare PC.
- Open Plex Web, go to Settings → General and read the version shown. The vendor says to look there.

```
dpkg -s plexmediaserver | grep Version
docker ps --format '{{.Names}} {{.Image}}' | grep -i plex
```

Step 2: Reduce exposure until it is patched

- If you cannot update today, take the server off the internet, for example by removing the router port forward. The vendor's warning concerns internet-facing servers.

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

Step 3: Update to the fixed version

- Move to 1.43.3.10861 or newer. The vendor says update instructions for each platform are in its original post.
- Check Settings → General again afterwards.

Step 4: Check for signs of compromise

- Look for processes started by Plex that you do not recognise, and for unfamiliar .so or .dll files in the Codecs folder.
- If you find any, follow the vendor's advice: rebuild clean, empty Codecs, check Preferences.xml, sign out all devices and change the password.

```
ps aux | grep -i plex
```

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. CISA lists CVE-2026-96652 in Plex Media Server as exploited, with a deadline of 3 November 2026. Please tell us whether we run Plex Media Server anywhere, and on which machines. For each one, we need the version and whether it can be reached from the internet. The vendor says versions before 1.43.3.10861 are affected and 1.43.3.10861 or later is not. Please update any older server and check it for signs of compromise, as the vendor describes. Please confirm in writing the version now running on each server and that the fix is in place, 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 Media Server that you do not recognise, such as 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.
- Outbound connections to proxystream.st, or sustained high CPU use while nothing is playing.

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 which could allow an attacker using any X-Plex-Token value to include a full URL in the 'protocol' parameter and force the Plex server to POST to the attacker's chosen destination. This vulnerability can be chained with CVE-2026-96654, CVE-2026-96655, and CVE-2026-96656.*

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

> *Plex Media Server before 1.43.3.10861 allows SSRF via '/player/timeline'. An attacker using any X-Plex-Token value can include a full URL in the 'protocol' parameter and force the Plex server to POST to the attacker's chosen destination.*

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 who is behind the attacks.
- The vendor's list of signs is examples (process names, a domain, Codecs files), not a complete list. A clean check does not prove a server is clean.
- The sources do not say what the Plex service account could reach on your network. That depends on your setup.
- The vendor's earlier release note warns that some app stores, such as QNAP, may be slow to offer an update. The sources do not say when each platform gets 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-2026-96652: 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

Server older than 1.43.3.10861, reachable from the internet	High	Today; CISA's deadline is 3 November 2026
Old version with signs of compromise, or you cannot rule it out	High	Immediately; rebuild as the vendor advises
Server older than 1.43.3.10861, reachable only on the local network	Medium	This week
Server already on 1.43.3.10861 or newer	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-2026-96652: https://www.cve.org/CVERecord?id=CVE-2026-96652
- 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-2026-96652
- Reference in the CVE record: zmain.info: https://zmain.info/blog/plex2shell