contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Plex Media Server exploited

CVE-2026-96654 · on CISA's exploited list since 20 October 2026

Analysis Report

If you run Plex Media Server older than 1.43.3.10861, update it now; CISA's date of 23 October 2026 has already passed. If it faces the internet, treat it as possibly compromised and check it. No …

PREPARED BY	NamiQ	DATE	1 November 2026
FACTS AS OF	1 November 2026	VERSION	1.0
SEVERITY	**Medium: CVSS 4.0 6.9**	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-2026-96654

The bottom line

> *If you run Plex Media Server older than 1.43.3.10861, update it now; CISA's date of 23 October 2026 has already passed. If it faces the internet, treat it as possibly compromised and check it. No Plex, nothing to do.*

At a glance

Fact	Detail
Product	Plex Media Server (CVE-2026-96654)
Severity	Medium: 6.9 (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 (the record and the vendor's post of 19 October 2026 both say so).
Who looks first	Anyone running Plex Media Server older than 1.43.3.10861, starting with servers reachable from the internet. Include machines where Plex was installed informally and that can reach shared storage.

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 on a spare PC, NAS or VM?	Nothing to do for this CVE.	Find the version (next question).
Is the version older than 1.43.3.10861?	You are on a fixed build. Still run the compromise checks if it was ever exposed.	Update, and treat it as exposed until checked.
Is the server reachable from the internet, for example with remote access on or port 32400 forwarded?	Lower risk, but update in the same week.	Update today and check for signs of compromise.

Can the Plex service account reach shares or stored credentials?	Damage is limited to the server itself.	If compromise is possible, treat those as exposed too.

What it is

The record says the server does not neutralize URL values in 'searchOne', so an attacker can call other plugins' functions and supply their own parameters. The vendor says this was chained with three other flaws to run code on the server without a login.

Why it matters

Our reading is that this flaw is a stepping stone. The vendor's post describes it as access to internal agent functions over the loopback interface, which the other three flaws build on to run code. The record's score of 6.9 therefore understates the risk. The vendor says the four together are being widely exploited, with cryptocurrency miners and proxy software installed on victims' servers. An owner who sees a media server as harmless may leave it unpatched, yet it runs with whatever access its service account has.

What the vendor's advisory says

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

- The vendor's 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.
- The vendor says chained together they let an unauthenticated remote attacker run code with the privileges of the Plex Media Server process.
- The vendor says a public proof of concept was released on 16 October and that attacks against internet-facing, unpatched servers are widespread.
- The vendor says a server older than 1.43.3.10861 and reachable from the internet should be assumed possibly compromised.
- The vendor's workaround advice: turn off remote access under Settings → Remote Access if not needed, and avoid forwarding port 32400 directly.

Things people will get wrong

- A 6.9 score means this can wait The vendor says this flaw is chained with three others and is being widely exploited. The score of one link does not describe the chain.
- Our server is only for media, so nothing of value is at risk The vendor says the service account's reach, such as mounted shares and stored credentials, should be treated as potentially exposed after a compromise.

- Updating removes anything an attacker already installed The vendor advises rebuilding from a clean installation if compromise cannot be ruled out. An update alone is not enough.

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

- Open Plex Web, go to Settings → General and read the version shown, as the vendor advises.
- Anything older than 1.43.3.10861 is affected. Check every host, VM and container that runs Plex.

```
dpkg -l plexmediaserver
rpm -q plexmediaserver
docker ps --format '{{.Names}} {{.Image}}'
```

Step 2: Reduce exposure

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

Step 3: Update to a fixed version

- Move to 1.43.3.10861 or newer, using the vendor's update instructions for your platform.
- Read the version again afterwards to confirm it.

Step 4: Check for signs of compromise

- Look for the signs in the next section. If you find any, or cannot rule it out, rebuild from a clean installation rather than reusing the old data directory.
- Sign out of all devices, change the Plex password and treat anything the service account could reach 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 have seen that Plex Media Server CVE-2026-96654 is being exploited and CISA's date of 23 October 2026 has passed. Please find out whether we run Plex Media Server anywhere, and on which hosts. Please tell us the version on each. The vendor says 1.43.3.10861 or later is not affected. If any host is older, please update it, turn off remote access if it is not needed, and check for signs of compromise. Please confirm in writing, by the end of this week, the version on each host and that the fix is in place.*

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, or sustained high CPU use while nothing is playing.
- Unfamiliar .so or .dll files in the Plex Codecs folder, or transcoder options in Preferences.xml that you did not set.
- Outbound connections from the server that you cannot explain, which the vendor links to proxy software.

The weakness behind it

The record classes this as CWE-84 (Improper Neutralization of Encoded URI Schemes in a Web Page).

The sources, in their words

CISA's catalogue entry:

> *Plex Media Server contains an improper neutralization of encoded URI schemes in a web page vulnerability that could allow an attacker to call other plugins' functions and supply their own parameters. This vulnerability can be chained with CVE-2026-96652, 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 does not correctly neutralize URL values included in 'searchOne,' allowing an attacker to call other plugins' functions and supply their own parameters.*

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 whether CVE-2026-96654 can be exploited on its own, without the other three flaws.
- The sources do not say whether servers reachable only from an internal network have been attacked.
- The vendor's post and the CSAF record describe CVE-2026-96655 differently (admin token disclosure versus a server-side request flaw).
- 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-2026-96654: score 6.9, `CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/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	None	No account is needed.
User interaction	None	No one has to do anything.
Vulnerable system: confidentiality	Low	Some data exposed.
Vulnerable system: integrity	Low	Some data or behaviour 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.
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

Server older than 1.43.3.10861 and reachable from the internet	High	Today; CISA's date has passed
Server older than 1.43.3.10861 on an internal network only	Medium	This week
Server on 1.43.3.10861 or later that was exposed while unpatched	Medium	This week: check for signs of compromise
Server on 1.43.3.10861 or later, never exposed	Low	Next patch cycle
No Plex Media Server in the estate	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-2026-96654: https://www.cve.org/CVERecord?id=CVE-2026-96654
- 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-2026-96654
- Reference in the CVE record: zmain.info: https://zmain.info/blog/plex2shell