

FOR IMMEDIATE RELEASE

October 22, 2026

Limehawk Urges Plex Media Server Owners to Update After Active Attacks

Plex says four chained flaws in older versions are being actively and widely exploited. Version 1.43.3.10861 fixes them.

KNOXVILLE, Tenn., Oct. 22, 2026. Limehawk, LLC, a Knoxville managed IT services provider, today urged businesses and their employees to update Plex Media Server to version 1.43.3.10861 or later and check for signs of compromise, after Plex warned that four flaws in older versions are being exploited.

On Oct. 19, Plex said: "These vulnerabilities are being actively and widely exploited. A public proof of concept was released on October 16." CISA added all four, CVE-2026-96652, CVE-2026-96654, CVE-2026-96655 and CVE-2026-96656, to its Known Exploited Vulnerabilities catalog on Oct. 20.

None of the four is rated critical on its own. The highest score listed in NVD is 8.6, High, under CVSS v4.0, for CVE-2026-96656. Plex says that "chained together, these issues let an unauthenticated remote attacker run code with the privileges of the Plex Media Server process."

Plex says it has seen "widespread attacks against internet-facing servers that haven't been updated," and that "compromised servers have been used to run cryptocurrency miners and proxy software, which routes other people's traffic through the victim's internet connection." Plex first announced the 1.43.3 update on Sept. 1.

Why does this matter for businesses?

Plex can run on office NAS devices and on home servers belonging to people who work remotely. Those machines can sit on the same network as file shares and stored credentials.

What should Plex owners do?

Limehawk recommends these steps:

- **Find every Plex server.** Check office NAS devices and servers, and ask remote staff whether they run Plex at home.
- **Update now.** Plex says to confirm the server is on 1.43.3.10861 or newer under Settings > General in Plex Web. On a NAS, Plex says you may need to install the package manually.
- **Assume exposure if you were behind.** Plex says: "If your server is older than 1.43.3.10861 and reachable from the internet, assume it may be compromised."

- **Check for signs of compromise.** Plex lists processes started by Plex Media Server that you don't recognize, "especially names like myawesomeproxy, mylovelyminer or x12345"; unfamiliar .so or .dll files in the Plex Codecs folder; and outbound connections to proxystream.st, or sustained high CPU use while nothing is playing.
- **Turn off Remote Access if you don't need it.** Plex says to disable it under Settings > Remote Access and to avoid forwarding port 32400 directly unless you need it.

What if a server was compromised?

Plex says to rebuild the server from a clean installation rather than reusing the old Plex data directory. At minimum, delete everything in the Codecs folder and check Preferences.xml for transcoder options you didn't set. Sign out of all devices from your Plex account settings and change your Plex password. Plex also says to treat anything the Plex service account could reach as potentially exposed, such as mounted shares and credentials stored on the same machine or VM.

Sources

1. Plex, "Important Security Update for Plex Media Server v1.43.2 and earlier." Updated Oct. 19, 2026.
<https://forums.plex.tv/t/important-security-update-for-plex-media-server-v1-43-2-and-earlier/942319>
2. CISA, "CISA Adds Six Known Exploited Vulnerabilities to Catalog." Oct. 20, 2026.
<https://www.cisa.gov/news-events/alerts/2026/10/20/cisa-adds-six-known-exploited-vulnerabilities-catalog>
3. NVD, "CVE-2026-96652." Published Sept. 23, 2026.
<https://nvd.nist.gov/vuln/detail/CVE-2026-96652>
4. NVD, "CVE-2026-96654." Published Sept. 23, 2026.
<https://nvd.nist.gov/vuln/detail/CVE-2026-96654>
5. NVD, "CVE-2026-96655." Published Sept. 23, 2026.
<https://nvd.nist.gov/vuln/detail/CVE-2026-96655>
6. NVD, "CVE-2026-96656." Published Sept. 23, 2026.
<https://nvd.nist.gov/vuln/detail/CVE-2026-96656>

Media Contact

Corey Watson, Managing Member
Limehawk, LLC
press@limehawk.io
<https://limehawk.io>

###