

PSA: Patch your Plex media server before someone hacks it

Recently fixed vulnerabilities in the Plex Media Server are under active exploitation in attacks that, when successful, install malware, including cryptominers and residential proxy apps, a researcher said.

Plex fixed four vulnerabilities at the start of last month. Three weeks later, published CVE designations revealed five vulnerabilities, with one of them carrying a severity rating of 8.6 out of 10. A researcher last week revealed an exploit that chained four of them together to achieve remote code execution of the device running a vulnerable Plex version. The researcher named the chain "Plex2Shell."

Complex exploit chain

The new details allowed a separate researcher to create a honeypot that could track attempts in the wild to exploit the vulnerability chain. Within a day, the researcher began seeing active scanning of the simulated Plex server and eventually successful attempts to infect devices. So far, successful attacks are installing two payloads. One is a cryptominer, which uses the device to mine cryptocurrency and deposit it into a wallet controlled by the attacker. The other payload is residential proxy software, which allows people to anonymize their Internet activity (much of it illegal) by connecting to the infected box and then using it to send the user's traffic to a final destination.

[Read full article](#)

Comments

<https://arstechnica.com/security/2026/10/recently-fixed-plex-media-vulnerabilities-are-being-exploited-to-install-malware/>