SERVICE ALERT

Prepared Nov 27, 2026, 5:31 PM PST

CloudLinux: CVE-2026-123007 NGINX2Root: unauthenticated HTTP/2 remote code execution in nginx

Status: Ongoing

Started Nov 18, 2026, 12:00 PM PST · CloudLinux's estimate: nginx fixes out now; CloudLinux 9.9 reaches 9.8 servers in batches over about two weeks from November 16; kernel SCTP fix: no CloudLinux date published

WHAT HAPPENED

CloudLinux has released fixed nginx packages for the nginx2root flaws, and servers already updated on November 18 should update again. A separate kernel flaw that can be chained with these bugs still has no CloudLinux fix, so we are keeping the risk-reducing steps in place. We will send the next update when CloudLinux publishes a kernel fix.

DOES THIS AFFECT YOU?

Servers running nginx with HTTP/2 turned on can be attacked over the internet to run code, and one government agency reports attacks, which other sources have not confirmed. If BIS manages your server, we are checking its nginx build for you.

WHAT BIS IS DOING

We are checking the nginx builds on the servers we manage against CloudLinux's fixed-build table. We will send the next update when CloudLinux reports a kernel fix.

WHAT YOU NEED TO DO

Update nginx again if you installed it on November 18, then restart it. CloudLinux 9.8 servers on nginx 1.26 should take the 9.9 update once it reaches them.

IS THIS A HACK?

Not confirmed — an attack has been suggested, but the vendor has not confirmed it.

LATEST UPDATES

Nov 27, 2026, 5:31 PM PST

New: the Imunify360 WebShield bundle has a fixed build (1.50.1-3) on CloudLinux's own blog; the CloudLinux nginx2root advisory is unchanged and still has no kernel fix.

Nov 27, 2026, 5:29 PM PST

CloudLinux's November 19 advisory lists fixed nginx packages for CloudLinux OS 9, and public exploit reports are now on record.

Nov 27, 2026, 4:05 PM PST

New: a news report says an upstream Linux kernel fix for the SCTP flaw landed on November 22; it is unconfirmed, and CloudLinux's advisory still shows no kernel build.

WHAT THE IT COMMUNITY IS SAYING

Only one post in the last seven days is clearly on this topic: a repost on X (about 4 days old) saying Palo Alto Networks confirmed the HTTP/2 nginx flaws affect PAN-OS and Panorama, with workarounds. Nearly all the other discussion I found is from November 18–19, outside the window, and none of the in-window posts report breakage, a working fix, or a CloudLinux-specific update.

From public posts by IT administrators; not confirmed by the vendor.

For technical details (versions, patches and sources), ask BIS for the Technical brief.

Questions? Contact BIS Computer Solutions, Inc.

Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com