SERVICE ALERT

Prepared Nov 27, 2026, 5:29 PM PST

CentOS Linux: CVE-2026-99362 NFS2ROOT: Linux kernel nfsd remote root flaw

Status: Ongoing

Started Nov 19, 2026, 6:24 AM PST

WHAT HAPPENED

A serious Linux kernel flaw affects servers that share files over NFS. We are checking whether your server runs NFS and whether its kernel has a fix, and we will tell you what to install. If your server shares files over NFS, please tell us so we can prioritise it.

DOES THIS AFFECT YOU?

If you use the affected service, you may notice problems. BIS is checking the systems we manage for you.

WHAT BIS IS DOING

We are watching for a fixed build for the CentOS 7 kernel on your server and will send the next update when one is confirmed.

WHAT YOU NEED TO DO

Confirm whether your server serves NFS; if it does, limit port 2049 until a fixed kernel is installed.

IS THIS A HACK?

No — this is not a hack or cyberattack.

LATEST UPDATES

Nov 27, 2026, 5:29 PM PST

New: Debian, Red Hat and Ubuntu status, the exploitation picture and the upstream stable branches are now reported, but no source names a fixed build for the CentOS 7 kernel 6.14.3-linode168.

Nov 27, 2026, 5:25 PM PST

New: third-party summaries report fixed kernels for RHEL 8.6 extended life and Rocky Linux 8, and one third-party source says Red Hat lists the RHEL 7 kernel as affected. Still no CentOS 7 kernel fix.

Nov 27, 2026, 3:17 PM PST

One new item: cve.now lists a public proof-of-concept exploit and a fix version, both conflicting with earlier reports and unconfirmed. There is still no CentOS 7 fix.

WHAT THE IT COMMUNITY IS SAYING

Posts from Nov 23 to 27 mostly pass along OpenSec's write-up, with its four fixed-kernel branches and advice to restrict tcp/2049 or turn off NFSv4.1 and 4.2, plus host-side hunting indicators. A Hacker News commenter says the bug was patched months ago, and Pillitteri says the CVE record lists more fixed branches than OpenSec does. I found no post from a CentOS 7 or RHEL 7 admin, no breakage report, no fix confirmation, and no in-the-wild exploitation report.

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