SERVICE ALERT

Prepared Nov 27, 2026, 5:25 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 flaw in the Linux file-sharing service (NFS) can let someone on the network take over a server that offers NFS. Servers that do not share files over NFS are not affected. No fix for CentOS 7 has been published yet, so BIS is checking your CentOS 7 servers now and will tell you before we change anything that affects your files.

DOES THIS AFFECT YOU?

Servers that share files over NFS and are reachable on port 2049 are affected. Machines that only mount NFS shares are not affected.

WHAT BIS IS DOING

We are checking CentOS 7 hosts that serve NFS and will apply the stopgap on any that do. We will send the next update when a fixed kernel for CentOS 7 is announced.

WHAT YOU NEED TO DO

If your server shares files over NFS, tell us so we can restrict port 2049 now. Otherwise nothing for now.

IS THIS A HACK?

No — this is not a hack or cyberattack.

LATEST UPDATES

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.

Nov 27, 2026, 11:15 AM PST

Minor new detail only: Tenable's unpatched-package plugin also lists CentOS 7 and RHEL 7 targets; there is still no CentOS 7 kernel 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