TECHNICAL BRIEF

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

WHERE THINGS STAND

CVE-2026-99362 (NFS2ROOT) is public: a pre-auth memory-corruption flaw in the Linux kernel NFS server, reachable on tcp/2049 for NFSv4.1/4.2. Upstream fixes exist in 6.12.117, 6.18.61, 7.3.2 and 7.4-rc1, but no source names a fixed build for the CentOS 7 kernel 6.14.3-linode168.

Affected: Linux kernel nfsd (NFSv4.1 and 4.2), CentOS Linux 7.9.2009, kernel 6.14.3-x86_64-linode168 (unconfirmed), Debian 12 linux-6.12 (fixed) and default 6.1 kernel (still vulnerable), Ubuntu 22.04 and 24.04 (no fix yet, unconfirmed), RHEL 6 to 10 (secondary report)

REFERENCE NUMBERS

ID	TYPE	SEVERITY	EXPLOITED	LINK
CVE-2026-99362	CVE	CVSS 9.8 · critical	No	https://cve.org/CVERecord/?id=CVE-2026-99362

AFFECTED VERSIONS AND FIXES

Every publicly affected version line found. Rows marked (BIS) are systems BIS runs.

PRODUCT / DISTRIBUTION	AFFECTED	FIXED IN	STATUS	SOURCE
(BIS) CentOS Linux 7.9.2009, kernel 6.14.3-x86_64-linode168	6.14.3 (no 6.14 line in any fixed list)	—	UNCONFIRMED	none found
Debian 12 default linux 6.1	6.1.192-2	—	WAITING	getrff (secondary report), 2026-11-25
Ubuntu 22.04 and 24.04	current kernels	—	UNCONFIRMED	getrff (secondary report), 2026-11-25
RHEL 6 to 10 and OpenShift 4/5 images	kernel packages listed as Affected	—	UNCONFIRMED	Red Hat rating as reported by BreachNews (Red Hat page not opened), 2026-11-25
Linux kernel upstream 6.12.y	before 6.12.117	6.12.117	FIXED	kernel.org changelog (via tldrcve), 2026-11-10
Linux kernel upstream 6.18.y	before 6.18.61	6.18.61	FIXED	kernel.org changelog (via tldrcve), 2026-11-06
Linux kernel 7.3.y	before 7.3.2	7.3.2	FIXED	kernel.org changelog (via tldrcve), 2026-11-06
Linux mainline	before 7.4-rc1	7.4-rc1	FIXED	OpenSec / tldrcve
Debian 12 linux-6.12	before 6.12.117-1~deb12u1	6.12.117-1~deb12u1	FIXED	Debian DLA-4927-1 (secondary report)

Questions? Contact BIS Computer Solutions, Inc.

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

WORKAROUNDS UNTIL A FIX IS INSTALLED

- Limit tcp/2049 to trusted storage hosts at the firewall.
- Disable NFSv4.1 and 4.2 (for example echo -4.1 and -4.2 to /proc/fs/nfsd/versions, or /etc/nfs.conf.d, then restart nfs-server); NFSv4.0 and NFSv3 are not reachable by this path.

HOW TO CHECK IF A SYSTEM IS AFFECTED

```
uname -r
cat /proc/fs/nfsd/threads (above 0 means NFS is serving)
cat /proc/fs/nfsd/versions (look for +4.1 or +4.2)
```

ROOT CAUSE

The NFSv4.1 SEQUENCE handler narrows the reply buffer to the session's cached reply limit before accepting the slot; a client can negotiate the limit down to a minimum, so the server writes past a zero-length slot buffer. The upstream fix adds a preflight size check.

EXPLOITATION

Not confirmed exploited: OpenSec says it built a root shell but keeps the exploit private; tldrcve and cve.now report no attacks seen; CISA KEV had not listed it as of 25 Nov 2026 (brandefense).

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.

TIMELINE (NEWEST FIRST)

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.

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.

Nov 27, 2026, 7:13 AM PST

GetPageSpeed now names a newer third-party kernel-lt build (6.18.65-1.el7) and says Red Hat lists the RHEL 7 kernel as affected; still no CentOS 7 fix.

Nov 27, 2026, 3:11 AM PST

A third-party kernel packager says the stock CentOS 7 kernel gets no fix and that its own newer kernel carries the patch; no CentOS or Red Hat CentOS 7 kernel fix has been published.

Nov 26, 2026, 11:09 PM PST

Red Hat and AlmaLinux shipped RHEL 8 kernel fixes for CVE-2026-99362 on 2026-11-26, but no CentOS 7 fix has been found.

Nov 26, 2026, 7:07 PM PST

Scanner and tracker sources now flag CentOS kernel packages as unpatched and Red Hat lists RHEL 6 to 10 with no shipped errata, but there is still no CentOS 7 fix for the 6.14 kernel.

Nov 26, 2026, 3:05 PM PST

New since the last check: a national CERT advisory listing fixed kernel ranges (reported by Mallory), the kernel

CVE announcement with fix commits, and new detection guidance. Still no CentOS 7 kernel fix.

Nov 26, 2026, 11:03 AM PST

New since the staff note: the kernel CVE record and Red Hat's CVE page are now confirmed, Red Hat's mitigation steps are published, and no CentOS 7 fix or exploit has been reported; the CentOS 7 kernel's applicability is still unconfirmed.

Nov 24, 2026, 4:00 PM PST

OpenSec publishes research; exploit kept private (BreachNews)

Nov 19, 2026, 6:24 AM PST

CVE-2026-99362 published with stable fixes (Linux kernel CVE team)

Sep 21, 2026, 5:00 PM PDT

OpenSec reports bug to NFSD maintainers (OpenSec)

Aug 16, 2026, 5:00 PM PDT

Upstream fix sent by ANSSI (OpenSec)

SOURCES

tldrcve — https://tldrcve.com/nfs2root/
getrff — https://getrff.com/blog/nfs2root-cve-2026-99362-linux-nfs-server/
Linux kernel CVE announcement — https://lists.openwall.net/linux-cve-announce/2026/11/19/36
BreachNews — https://breachnews.com/research/nfs2root-cve-2026-99362-linux-nfsd-pre-auth-root/