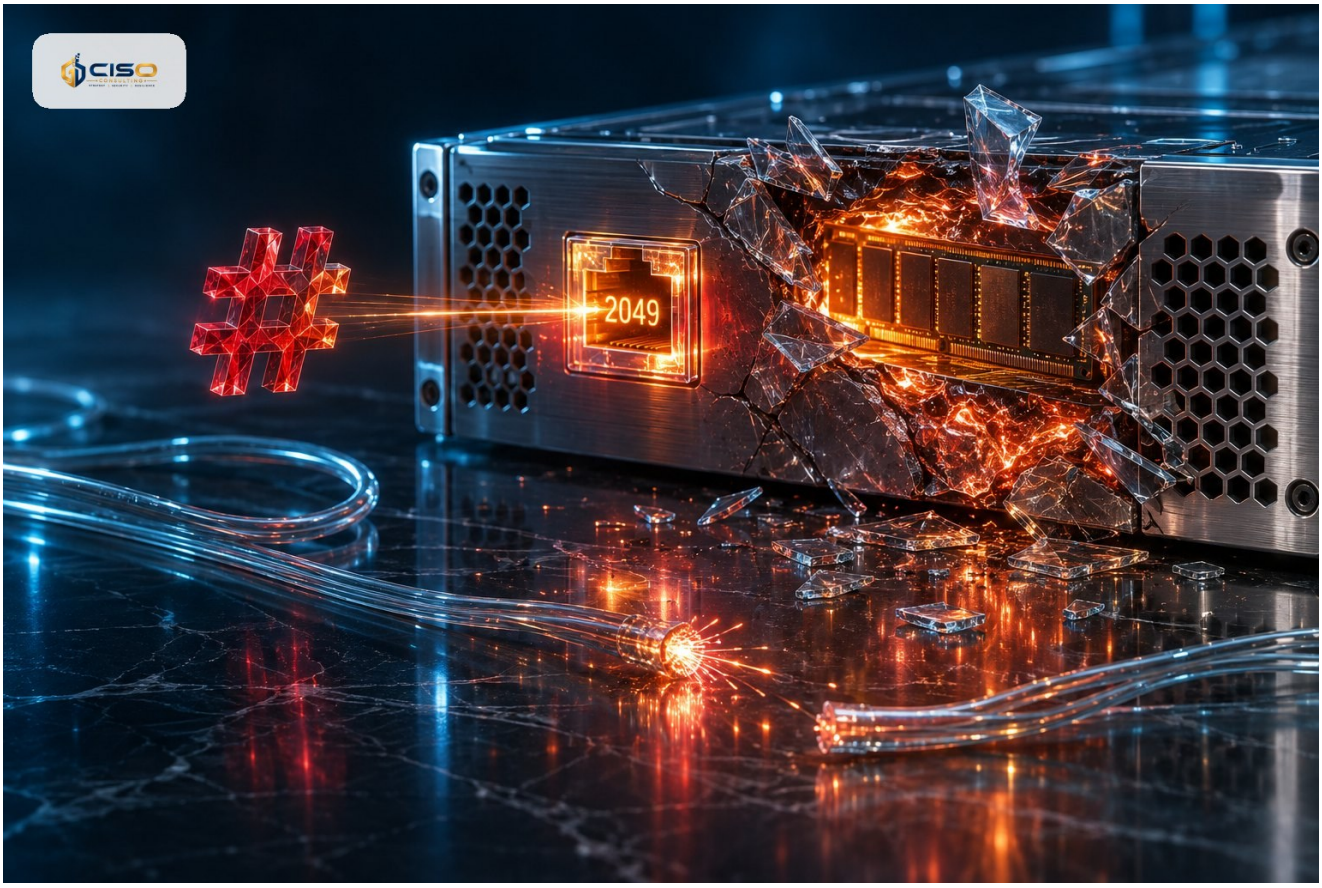
NFS2ROOT: Critical Linux NFS Server Flaw Allows Remote Root Access



A critical heap overflow in the Linux kernel NFS server, CVE-2026-99362, can give remote attackers root access when nfsd is running and port 2049 is reachable. No exploitation in the wild is reported.

- CVE-2026-99362, named NFS2ROOT, is a heap buffer overflow in the Linux kernel NFS server (nfsd) present since kernel 3.16.
- Affected: kernels older than 6.12.117, 6.18.61, 7.3.2 or 7.4-rc1 with nfsd (v4.1 or 4.2) running and TCP port 2049 reachable over the Internet.
- Attacks are low complexity, need no privileges or user interaction, and can bypass KASLR to run commands as root.
- No in-the-wild exploitation has been reported, but OpenSec shared a full exploit and a patch with

> the NFSD maintainers.
>
> - Mitigations: patch and reboot, restrict port 2049 to trusted clients, or disable nfs-server if not needed.

A critical vulnerability in the Linux kernel's NFS server, tracked as CVE-2026-99362 and named NFS2ROOT, can allow a remote attacker with no privileges to take root control of a server. It was found by Jérémy Jean of ANSSI, who submitted a fix in August. Security firm OpenSec shared a full exploit and a patch with the NFSD maintainers in late September.

What is affected

The flaw is a heap buffer overflow in nfsd that has existed since kernel 3.16, released in March 2014. Systems are exposed if they run a kernel older than 6.12.117, 6.18.61, 7.3.2 or 7.4-rc1, have nfsd (v4.1 or 4.2) loaded and running, and have TCP port 2049 reachable over the Internet.

An attacker sends crafted requests that make the server write beyond its allocated buffer. This allows kernel memory to be read, KASLR to be bypassed, and a command to be planted that the kernel runs as root when the attacker closes the connection. No user interaction is needed. There are no reports of exploitation in the wild so far.

Mitigation and detection

The recommended step is to apply the latest kernel security update from the distribution vendor and reboot so the patched kernel is active. Where patching must wait, access to port 2049 should be limited to trusted clients or networks, or the nfs-server service can be stopped and disabled if NFS sharing is not needed.

OpenSec notes the attacks have no network signatures. Possible signs include kernel warnings from nfsd4_check_resp_size, shells spawned by kernel workers on a file server, bursts of short NFSv4.1 sessions from one source, and kernel oopses with nfsd4_*, svc_* or call_usermodehelper* frames.

What to do now

1. Inventory Linux servers, NAS appliances, build hosts and Kubernetes storage nodes running nfsd, and check kernel versions against the fixed releases.
2. Confirm whether TCP port 2049 is reachable from the Internet and close or restrict it to trusted networks immediately.
3. Apply the vendor kernel security update and reboot, then verify the patched kernel is running.
4. Where patching is delayed, disable nfs-server on hosts that do not need NFS sharing.
5. Add the OpenSec indicators (nfsd4_check_resp_size warnings, shells from kernel workers, bursts of short NFSv4.1 sessions) to monitoring and review recent logs.

6. Record the exposure and remediation under your vulnerability management process for NCA and SAMA reporting needs.