nfsd: fix heap overflow in NFSv4.0 LOCK replay cache

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-31402
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-03 16:16:39 UTC
Updated	2026-04-03 16:16:39 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix heap overflow in NFSv4.0 LOCK replay cache Th

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 c9452c0797c95cf2378170df96cf4f4b3bca7eff git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 8afb437ea1f70cacb4bbdf11771fb5c4d720b965 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 dad0c3c0a8e5d1d6eb0fc455694ce3e25e6c57d0 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 0f0e2a54a31a7f9ad2915db99156114872317388 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ae8498337dfdfda71bdd0b807c9a23a126011d76 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 5133b61aaf437e5f25b1b396b14242a6bb0508e2 git
CNA	Linux	Linux	affected 2.6.12
CNA	Linux	Linux	unaffected 2.6.12 semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.20 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.10 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc5 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/5133b61aaf437e5f25b1b396b14242a6bb0508e2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8afb437ea1f70cacb4bbdf11771fb5c4d720b965	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/dad0c3c0a8e5d1d6eb0fc455694ce3e25e6c57d0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	

git.kernel.org/stable/c/0f0e2a54a31a7f9ad2915db99156114872317388	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c9452c0797c95cf2378170df96cf4f4b3bca7eff	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ae8498337dfdfda71bdd0b807c9a23a126011d76	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.