



NFSD: Hold net reference for the lifetime of /proc/fs/nfs/exports fd

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2026-31403
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: Hold net reference for the lifetime of /proc/fs/nfs/ex

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 96d851c4d28de8cc83fe2bd5c6bc2eb8f253a6c5 c7f406fb341d6747634b8b1fa5461656e5e56076 git
CNA	Linux	Linux	affected 96d851c4d28de8cc83fe2bd5c6bc2eb8f253a6c5 d1a19217995df9c7e4118f5a2820c5032fef2945 git
CNA	Linux	Linux	affected 96d851c4d28de8cc83fe2bd5c6bc2eb8f253a6c5 e3d77f935639e6ae4b381c80464c31df998d61f4 git
CNA	Linux	Linux	affected 96d851c4d28de8cc83fe2bd5c6bc2eb8f253a6c5 db4a9f99b12a7ee1c19d86c83a3b752c7effa6c6 git
CNA	Linux	Linux	affected 96d851c4d28de8cc83fe2bd5c6bc2eb8f253a6c5 6a8d70e2ad6aad2c345a5048edcb8168036f97d6 git
CNA	Linux	Linux	affected 96d851c4d28de8cc83fe2bd5c6bc2eb8f253a6c5 e7fcf179b82d3a3730fd8615da01b087cc654d0b git
CNA	Linux	Linux	affected 3.9
CNA	Linux	Linux	unaffected 3.9 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/db4a9f99b12a7ee1c19d86c83a3b752c7effa6c6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e3d77f935639e6ae4b381c80464c31df998d61f4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	

git.kernel.org/stable/c/e7fcf179b82d3a3730fd8615da01b087cc654d0b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/c7f406fb341d6747634b8b1fa5461656e5e56076	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6a8d70e2ad6aad2c345a5048edcb8168036f97d6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d1a19217995df9c7e4118f5a2820c5032fef2945	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report