nsfs: tighten permission checks for ns iteration ioctls

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-43403
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:51 UTC
Updated	2026-05-11 08:16:13 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: nsfs: tighten permission checks for ns iteration ioctls Even

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

EPSS: 0.000180000 probability, percentile 0.047390000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected a1d220d9dafa8d76ba60a784a1016c3134e6a1e8 3376b345df155ca36d8611857b41ff7d5183fc38 git
CNA	Linux	Linux	affected a1d220d9dafa8d76ba60a784a1016c3134e6a1e8 2f3dea284c761c890d676f77d5e55c0c496b4ef4 git
CNA	Linux	Linux	affected a1d220d9dafa8d76ba60a784a1016c3134e6a1e8 0ad650e60150eda789deca5e78a6a09d26bf8fc9 gi
CNA	Linux	Linux	affected a1d220d9dafa8d76ba60a784a1016c3134e6a1e8 e6b899f08066e744f89df16ceb782e06868bd148 git
CNA	Linux	Linux	affected 6.12
CNA	Linux	Linux	unaffected 6.12 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 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/3376b345df155ca36d8611857b41ff7d5183fc38	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e6b899f08066e744f89df16ceb782e06868bd148	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/0ad650e60150eda789deca5e78a6a09d26bf8fc9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/2f3dea284c761c890d676f77d5e55c0c496b4ef4	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.

Free CVE JSON API cve.report/api

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