ksmbd: fix use-after-free in __ksmbd_close_fd() via durable scavenger

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

Summary

CVE	CVE-2026-31718
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:21 UTC
Updated	2026-05-03 07:16:18 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in __ksmbd_close_fd() via durab

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.046600000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected c8efcc786146a951091588e5fa7e3c754850cb3c e33c65f011980b4ad4abfd93585ec2079856368f git
CNA	Linux	Linux	affected c8efcc786146a951091588e5fa7e3c754850cb3c 3d6682726c2d3a46d31dae88b8166786b09b03ad gi
CNA	Linux	Linux	affected c8efcc786146a951091588e5fa7e3c754850cb3c b34fc42cfe922e551f7a27d3ac3bb016e41d7dd9 git
CNA	Linux	Linux	affected c8efcc786146a951091588e5fa7e3c754850cb3c 235e32320a470fcd3998fb3774f2290a0eb302a1 git
CNA	Linux	Linux	affected 8df4bcdb0a4232192b2445256c39b787d58ef14d git
CNA	Linux	Linux	affected 6.9
CNA	Linux	Linux	unaffected 6.9 semver
CNA	Linux	Linux	unaffected 6.12.84 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.25 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.2 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/3d6682726c2d3a46d31dae88b8166786b09b03ad	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b34fc42cfe922e551f7a27d3ac3bb016e41d7dd9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e33c65f011980b4ad4abfd93585ec2079856368f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/235e32320a470fcd3998fb3774f2290a0eb302a1	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.

Free CVE JSON API cve.report/api

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