ksmbd: fix use-after-free in smb_lazy_parent_lease_break_close()

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

Summary

CVE	CVE-2026-43379
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:49 UTC
Updated	2026-05-11 08:16:12 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in smb_lazy_parent_lease_break

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 0.049330000 (date 2026-05-10)

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 27b40b7bfcd121fe13a150ffe11957630cf49246 bf4d66d72e4a9e268c1012c331ce9eaedb5e2086 git
CNA	Linux	Linux	affected 5fb282ba4fef8985a5acf2b32681f2ec07732561 960699317d39f46611f4ebeb69edc567c1f4e6b6 git
CNA	Linux	Linux	affected 5fb282ba4fef8985a5acf2b32681f2ec07732561 dbbd328cf58261ca239756fe1c0d10c9518d3399 git
CNA	Linux	Linux	affected 5fb282ba4fef8985a5acf2b32681f2ec07732561 b3568347c51c46e2cabc356bc34676df98296619 git
CNA	Linux	Linux	affected 5fb282ba4fef8985a5acf2b32681f2ec07732561 eac3361e3d5dd8067b3258c69615888eb45e9f25 git
CNA	Linux	Linux	affected 6.9
CNA	Linux	Linux	unaffected 6.9 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 6.18.19 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/dbbd328cf58261ca239756fe1c0d10c9518d3399	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/bf4d66d72e4a9e268c1012c331ce9eaedb5e2086	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/eac3361e3d5dd8067b3258c69615888eb45e9f25	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/960699317d39f46611f4ebeb69edc567c1f4e6b6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b3568347c51c46e2cabc356bc34676df98296619	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.