ksmbd: fix use-after-free by using call_rcu() for oplock_info

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

Summary

CVE	CVE-2026-43376
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:48 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 by using call_rcu() for oplock_info

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 296cb5457cc6f4a754c4ae29855f8a253d52bcc6 302fef75512b2c8329a3f5efab1ae7ba2562387a git
CNA	Linux	Linux	affected d54ab1520d43e95f9b2e22d7a05fc9614192e5a5 08aa9f3c8cf4d0bee44df540dfe34e8d64069f2c git
CNA	Linux	Linux	affected 18b4fac5ef17f77fed9417d22210ceafd6525fc7 1d6abf145615dbfe267ce3b0a271f95e3780e18e git
CNA	Linux	Linux	affected 18b4fac5ef17f77fed9417d22210ceafd6525fc7 ce8507ee82c888126d8e7565e27c016308d24cde git
CNA	Linux	Linux	affected 18b4fac5ef17f77fed9417d22210ceafd6525fc7 1dfd062caa165ec9d7ee0823087930f3ab8a6294 git
CNA	Linux	Linux	affected d73686367ad68534257cd88a36ca3c52cb8b81d8 git
CNA	Linux	Linux	affected 6.15
CNA	Linux	Linux	unaffected 6.15 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/302fef75512b2c8329a3f5efab1ae7ba2562387a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1dfd062caa165ec9d7ee0823087930f3ab8a6294	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/08aa9f3c8cf4d0bee44df540dfe34e8d64069f2c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1d6abf145615dbfe267ce3b0a271f95e3780e18e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ce8507ee82c888126d8e7565e27c016308d24cde	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