smb: server: avoid double-free in smb_direct_free_sendmsg after smb_direct_flush_send_list()

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

Summary

CVE	CVE-2026-31608
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:40 UTC
Updated	2026-04-29 20:03:44 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: smb: server: avoid double-free in smb_direct_free_sendm

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 0.046080000 (date 2026-04-27)

Problem Types: CWE-415

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 5ef18a2e66f2f33fdac64437bddfb9fe6389fdc7 6968c91fab05b8fc4d6700e0cf34472bb422df25 git
CNA	Linux	Linux	affected 79242e7b6bc63efec28b7c235bc320806afce6c0 2ba03f46132b0d1a7bafb86e1ef61951a2254023 git
CNA	Linux	Linux	affected 34abd408c8ba24d7c97bd02ba874d8c714f49db1 830de6eeb9db4cb7e758201fb99328ef4ca4b032 gi
CNA	Linux	Linux	affected 34abd408c8ba24d7c97bd02ba874d8c714f49db1 84ff995ae826aa6bbcc6c7b9ea569ff67c021d72 git
CNA	Linux	Linux	affected 7.0
CNA	Linux	Linux	unaffected 7.0 semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0.1 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/6968c91fab05b8fc4d6700e0cf34472bb422df25	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/84ff995ae826aa6bbcc6c7b9ea569ff67c021d72	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/830de6eeb9db4cb7e758201fb99328ef4ca4b032	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2ba03f46132b0d1a7bafb86e1ef61951a2254023	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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**