ksmbd: use check_add_overflow() to prevent u16 DACL size overflow

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

Summary

CVE	CVE-2026-31704
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:20 UTC
Updated	2026-05-06 20:46:54 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: use check_add_overflow() to prevent u16 DACL s

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000180000 probability, percentile 0.048290000 (date 2026-05-05)

Problem Types: NVD-CWE-noinfo

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/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 e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 8d5729350b236896f51379588d9a690b7fafb8db git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 e1955a94b6f17f4b058afa955a6f187eb3ed7615 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 5e7b8f3c539d69b2ed5f2408e2f75e68ce7eef43 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 ef7902be3f215b6bf7babe4dc9dd9a7d57dad7a7 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 299f962c0b02d048fb45d248b4da493d03f3175d git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* 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/e1955a94b6f17f4b058afa955a6f187eb3ed7615	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ef7902be3f215b6bf7babe4dc9dd9a7d57dad7a7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/5e7b8f3c539d69b2ed5f2408e2f75e68ce7eef43	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/299f962c0b02d048fb45d248b4da493d03f3175d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/8d5729350b236896f51379588d9a690b7fafb8db	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