ksmbd: fix out-of-bounds write in smb2_get_ea() EA alignment

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

Summary

CVE	CVE-2026-31705
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:20 UTC
Updated	2026-05-03 07:16:17 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix out-of-bounds write in smb2_get_ea() EA alignı

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 0.048520000 (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 e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d ffbce350c6fd1e99116ea57383b9031717e36d3b git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 98f3de6ef4efbd899348d333f0902dc4ff14380c git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 790304c02bf9bd7b8171feda4294d6e62d32ae8f git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 922d48fe8c19f388ffa2f709f33acaae4e408de2 git
CNA	Linux	Linux	affected e2b76ab8b5c9327ab2dae6da05d0752eb2f4771d 30010c952077a1c89ecdd71fc4d574c75a8f5617 git
CNA	Linux	Linux	affected f2283680a80571ca82d710bc6ecd8f8beac67d63 git
CNA	Linux	Linux	affected 9f297df20d93411c0b4ddad7f88ba04a7cd36e77 git
CNA	Linux	Linux	affected 6.6
CNA	Linux	Linux	unaffected 6.6 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/790304c02bf9bd7b8171feda4294d6e62d32ae8f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/98f3de6ef4efbd899348d333f0902dc4ff14380c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/922d48fe8c19f388ffa2f709f33acaae4e408de2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/30010c952077a1c89ecdd71fc4d574c75a8f5617	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ffbce350c6fd1e99116ea57383b9031717e36d3b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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