ksmbd: validate EaNameLength in smb2_get_ea()

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

Summary

CVE	CVE-2026-31612
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 17:00:28 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate EaNameLength in smb2_get_ea() smb2_

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.048130000 (date 2026-04-27)

Problem Types: NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

None

Availability

None

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

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 4b73376feecb3b61172fe5b4ff42bbbb8531669d git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 551dfb15b182abad4600eaf7b37e6eb7000d5b1b git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 3363a770b193f555f29d76ddf4ced3305c0ccf6d git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 243b206bcb5a7137e8bddd57b2eec81e1ebd3859 g
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 dfc6878d14acafffbe670bf2576620757a10a3d8 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 66751841212c2cc196577453c37f7774ff363f02 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 6.12.83 6.12.* 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/3363a770b193f555f29d76ddf4ced3305c0ccf6d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/243b206bcb5a7137e8bddd57b2eec81e1ebd3859	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/551dfb15b182abad4600eaf7b37e6eb7000d5b1b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/dfc6878d14acafffbe670bf2576620757a10a3d8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/4b73376feecb3b61172fe5b4ff42bbbb8531669d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/66751841212c2cc196577453c37f7774ff363f02	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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**