smb3: fix for slab out of bounds on mount to ksmbd

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

Summary

CVE	CVE-2025-38728
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-09-04 16:15:42 UTC
Updated	2026-05-12 13:17:03 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: smb3: fix for slab out of bounds on mount to ksmbd With k

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from nvd@nist.gov

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

Problem Types: CWE-125

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/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 fe856be475f7cf5ffcde57341d175ce9fd09434b 9bdb8e98a0073c73ab3e6c631ec78877ceb
CNA	Linux	Linux	affected fe856be475f7cf5ffcde57341d175ce9fd09434b a0620e1525663edd8c4594f49fb75fe5be47
CNA	Linux	Linux	affected fe856be475f7cf5ffcde57341d175ce9fd09434b 8de33d4d72e8fae3502ec3850bd7b14e7c7
CNA	Linux	Linux	affected fe856be475f7cf5ffcde57341d175ce9fd09434b a542f93a123555d09c3ce8bc947f7b56ad8e
CNA	Linux	Linux	affected fe856be475f7cf5ffcde57341d175ce9fd09434b f6eda5b0e8f8123564c5b34f5801d6324303
CNA	Linux	Linux	affected fe856be475f7cf5ffcde57341d175ce9fd09434b 7d34ec36abb84fdfb6632a0f2cbda90379ae
CNA	Linux	Linux	affected 4.18
CNA	Linux	Linux	unaffected 4.18 semver
CNA	Linux	Linux	unaffected 6.1.149 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.103 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.43 6.12.* semver
CNA	Linux	Linux	unaffected 6.15.11 6.15.* semver
CNA	Linux	Linux	unaffected 6.16.2 6.16.* semver
CNA	Linux	Linux	unaffected 6.17 * original_commit_for_fix
ADP	Siemens	SIMATIC CN 4100	affected V5.0 custom

References

Reference	Source	Link
lists.debian.org/debian-lts-announce/2025/10/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org
git.kernel.org/stable/c/a542f93a123555d09c3ce8bc947f7b56ad8e6463	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/9bdb8e98a0073c73ab3e6c631ec78877ceb64565	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/7d34ec36abb84fdfb6632a0f2cbda90379ae21fc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	cert-portal.siemens.cc
git.kernel.org/stable/c/f6eda5b0e8f8123564c5b34f5801d63243032eac	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/a0620e1525663edd8c4594f49fb75fe5be4724b0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
git.kernel.org/stable/c/8de33d4d72e8fae3502ec3850bd7b14e7c7328b6	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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**