ksmbd: fix session use-after-free in multichannel connection

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

Summary

CVE	CVE-2025-22040
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-16 15:15:56 UTC
Updated	2026-04-06 14:29:37 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix session use-after-free in multichannel connecti

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from ADP

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

Problem Types: CWE-416 | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/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 0626e6641f6b467447c81dd7678a69c66f7746cf 596407adb9af1ee75fe7c7529607783d31b66e7f git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 3980770cb1470054e6400fd97668665975726737 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 9069939d762138e232a6f79e3e1462682ed6a17d git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 94c281721d4ed2d972232414b91d98a6f5bdb16b git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 7dfbd4c43eed91dd2548a95236908025707a8dfd git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf fa4cdb8cbca7d6cb6aa13e4d8d83d1103f6345db git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.1.134 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.87 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.23 6.12.* semver
CNA	Linux	Linux	unaffected 6.13.11 6.13.* semver
CNA	Linux	Linux	unaffected 6.14.2 6.14.* semver
CNA	Linux	Linux	unaffected 6.15 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/9069939d762138e232a6f79e3e1462682ed6a17d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/7dfbd4c43eed91dd2548a95236908025707a8dfd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/3980770cb1470054e6400fd97668665975726737	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/94c281721d4ed2d972232414b91d98a6f5bdb16b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
lists.debian.org/debian-lts-announce/2025/05/msg00045.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Mail
git.kernel.org/stable/c/596407adb9af1ee75fe7c7529607783d31b66e7f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc

git.kernel.org/stable/c/fa4cdb8cbca7d6cb6aa13e4d8d83d1103f6345db	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.