ksmbd: fix use-after-free in ksmbd_sessions_deregister()

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

Summary

CVE	CVE-2025-22041
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-04-16 15:15:56 UTC
Updated	2026-04-02 09:16:18 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in ksmbd_sessions_deregister()

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 f0eb3f575138b816da74697bd506682574742fcd git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf a8a8ae303a8395cbac270b5b404d85df6ec788f8 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf ca042cc0e4f9e0d2c8f86dd67e4b22f30a516a9b git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 8ed0e9d2f410f63525afb8351181eea36c80bcf1 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 33cc29e221df7a3085ae413e8c26c4e81a151153 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 15a9605f8d69dc85005b1a00c31a050b8625e1aa 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/8ed0e9d2f410f63525afb8351181eea36c80bcf1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/33cc29e221df7a3085ae413e8c26c4e81a151153	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/ca042cc0e4f9e0d2c8f86dd67e4b22f30a516a9b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/a8a8ae303a8395cbac270b5b404d85df6ec788f8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/f0eb3f575138b816da74697bd506682574742fcd	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/15a9605f8d69dc85005b1a00c31a050b8625e1aa	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	
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.