ksmbd: fix use-after-free in kerberos authentication

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-37924
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-05-20 16:15:29 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 kerberos authentication Setting

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

Problem Types: CWE-416

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	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	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

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

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 e34a33d5d7e87399af0a138bb32f6a3e95dd83d2 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf b44746356223842850 3cfba1c913261047772f90 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf e18c616718018dfc440e4a2d2b94e28fe91b1861 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 28c756738af44a404a91b77830d017bb0c525890 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf e86e9134e1d1c90a960dd57f59ce574d27b9a124 git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.1.138 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.90 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.28 6.12.* semver
CNA	Linux	Linux	unaffected 6.14.6 6.14.* semver
CNA	Linux	Linux	unaffected 6.15 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/e18c616718018dfc440e4a2d2b94e28fe91b1861	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/e34a33d5d7e87399af0a138bb32f6a3e95dd83d2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/28c756738af44a404a91b77830d017bb0c525890	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
lists.debian.org/debian-lts-announce/2025/08/msg00010.html	af854a3a-2127-422b-91ae-364da2661108	lists.debian.org	Maili
git.kernel.org/stable/c/e86e9134e1d1c90a960dd57f59ce574d27b9a124	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patc
git.kernel.org/stable/c/b44746356223842850 3cfba1c913261047772f90	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.

CVE.report and Source URL Uptime Status status.cve.report