ksmbd: ipc: fix use-after-free in ipc_msg_send_request

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-68263
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-12-16 15:15:55 UTC
Updated	2026-04-02 09:16:19 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: ipc: fix use-after-free in ipc_msg_send_request ipc

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

Version	Source	Type	Score	Severity	Vector
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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf de85fb58f9967ba024bb08e0041613d37b57b4d1 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 708a620b471a14466f1f52c90bf3f65ebdb31460 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 5ac763713a1ef8f9a8bda1dbd81f0318d67baa4e git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 759c8c30cfa8706c518e56f67971b1f0932f4b9b git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 8229c6ca50cea701e25a7ee25f48441b582ec5fa git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 1fab1fa091f5aa97265648b53ea031deedd26235 git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.1.160 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.120 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.62 6.12.* semver
CNA	Linux	Linux	unaffected 6.17.12 6.17.* semver
CNA	Linux	Linux	unaffected 6.18.1 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/de85fb58f9967ba024bb08e0041613d37b57b4d1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/759c8c30cfa8706c518e56f67971b1f0932f4b9b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1fab1fa091f5aa97265648b53ea031deedd26235	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/708a620b471a14466f1f52c90bf3f65ebdb31460	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/5ac763713a1ef8f9a8bda1dbd81f0318d67baa4e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8229c6ca50cea701e25a7ee25f48441b582ec5fa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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