ksmbd: validate response sizes in ipc_validate_msg()

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

Summary

CVE	CVE-2026-31707
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:20 UTC
Updated	2026-05-03 07:16:18 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate response sizes in ipc_validate_msg() ipc_

Risk And Classification

Primary CVSS: v3.1 7.1 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.046600000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H
3.1	CNA	DECLARED	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 7dd0c858e1909769a4c91842724315ee74f1a5f1 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 299db777ea0cfa5c407e41b045c24a14c034c27b git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 99c631d0366c1eab8fb188fe66425f4581ebdde4 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf d6a6aa81eac2c9bff66dc6e191179cb69a14426b git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.12.84 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.25 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.2 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/299db777ea0cfa5c407e41b045c24a14c034c27b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d6a6aa81eac2c9bff66dc6e191179cb69a14426b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7dd0c858e1909769a4c91842724315ee74f1a5f1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/99c631d0366c1eab8fb188fe66425f4581ebdde4	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.

Free CVE JSON API cve.report/api

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