ksmbd: fix infinite loop caused by next_smb2_rcv_hdr_off reset in error paths

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

Summary

CVE	CVE-2026-23220
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-18 16:22:31 UTC
Updated	2026-04-18 09:16:14 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix infinite loop caused by next_smb2_rcv_hdr_off

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-835

CVSS v3.1 Breakdown

Attack Vector
Local

Attack Complexity
Low

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
None

Integrity
None

Availability
High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/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 4b9b7ea1ffb1e34f01fa5726d0c184931b9ba565 544adb0a6658ea1bff4064723761dbf05f95b1e2 git
CNA	Linux	Linux	affected 943cebf9ea3415ddefcd670d24d8883e97ba3d60 fb3b66bd72deb5543addaefa67963b34fb163a7b git
CNA	Linux	Linux	affected be0f89d4419dc5413a1cf06db3671c9949be0d52 5accdc5b7f28a81bbc5880ac0b8886e60c86e8c8 git
CNA	Linux	Linux	affected be0f89d4419dc5413a1cf06db3671c9949be0d52 f7b1c2f5642bbd60b1beef1f3298cbac81eb232c git
CNA	Linux	Linux	affected be0f89d4419dc5413a1cf06db3671c9949be0d52 71b5e7c528315ca360a1825a4ad2f8ae48c5dc16 git
CNA	Linux	Linux	affected be0f89d4419dc5413a1cf06db3671c9949be0d52 9135e791ec2709bcf0cda0335535c74762489498 git
CNA	Linux	Linux	affected be0f89d4419dc5413a1cf06db3671c9949be0d52 010eb01ce23b34b50531448b0da391c7f05a72af git
CNA	Linux	Linux	affected 6.6
CNA	Linux	Linux	unaffected 6.6 semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.164 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.125 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.72 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.11 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.1 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/5accdc5b7f28a81bbc5880ac0b8886e60c86e8c8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/544adb0a6658ea1bff4064723761dbf05f95b1e2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/fb3b66bd72deb5543addaefa67963b34fb163a7b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/010eb01ce23b34b50531448b0da391c7f05a72af	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f7b1c2f5642bbd60b1beef1f3298cbac81eb232c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/9135e791ec2709bcf0cda0335535c74762489498	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/71b5e7c528315ca360a1825a4ad2f8ae48c5dc16	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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**