smb: client: fix in-place encryption corruption in SMB2_write()

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

Summary

CVE	CVE-2026-43362
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:47 UTC
Updated	2026-05-11 08:16:11 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix in-place encryption corruption in SMB2_wri

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000100000 probability, percentile 0.012390000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 026e93dc0a3eefb0be060bcb9ecd8d7a7fd5c398 438e77435aee2894d5edf90be5c87004a57f6258 git
CNA	Linux	Linux	affected 026e93dc0a3eefb0be060bcb9ecd8d7a7fd5c398 52327268224fb9ccc7ecfbbdfdfff54b6e93c518 git
CNA	Linux	Linux	affected 026e93dc0a3eefb0be060bcb9ecd8d7a7fd5c398 92e64f1852f455f57d0850989e57c30d7fac7d95 git
CNA	Linux	Linux	affected 026e93dc0a3eefb0be060bcb9ecd8d7a7fd5c398 aea5e37388a080361110ab5790f57ae0af383650 git
CNA	Linux	Linux	affected 026e93dc0a3eefb0be060bcb9ecd8d7a7fd5c398 d78840a6a38d312dc1a51a65317bb67e46f0b929 gi
CNA	Linux	Linux	affected 4.11
CNA	Linux	Linux	unaffected 4.11 semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/aea5e37388a080361110ab5790f57ae0af383650	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/52327268224fb9ccc7ecfbbdfdfff54b6e93c518	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/438e77435aee2894d5edf90be5c87004a57f6258	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/92e64f1852f455f57d0850989e57c30d7fac7d95	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d78840a6a38d312dc1a51a65317bb67e46f0b929	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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