



ksmbd: fix memory leaks and NULL deref in smb2_lock()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-31477
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 14:16:44 UTC
Updated	2026-04-22 14:16:44 UTC

Description In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix memory leaks and NULL deref in smb2_lock() :

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 cdac6f7e7e428dc70e3b5898ac6999a72ed13993 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 c9b95ef6f5039f19e46c3a521a4fe1752d91dfe9 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 91aeea7256006d79a37298f5a1df23325db91599 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 3cdacd11b41569ce75b3162142240f2355e04900 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 aab42f0795620cf0d3955a520f571f697d0f9a2a git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 309b44ed684496ed3f9c5715d10b899338623512 git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.1.168 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.131 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.80 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.21 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.11 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/c9b95ef6f5039f19e46c3a521a4fe1752d91dfe9	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/cdac6f7e7e428dc70e3b5898ac6999a72ed13993	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	

git.kernel.org/stable/c/91aeaa7256006d79a37298f5a1df23325db91599	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/aab42f0795620cf0d3955a520f571f697d0f9a2a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/3cdacd11b41569ce75b3162142240f2355e04900	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/309b44ed684496ed3f9c5715d10b899338623512	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.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

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