



smb: client: fix off-by-8 bounds check in check_wsl_eas()

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

Summary

CVE	CVE-2026-31614
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:40 UTC
Updated	2026-04-24 17:51:40 UTC

Description In the Linux kernel, the following vulnerability has been resolved: smb: client: fix off-by-8 bounds check in check_wsl_eas()

Risk And Classification

EPSS: 0.000180000 probability, percentile 0.046210000 (date 2026-04-25)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 5cc0574c84aa73946ade587c41e81757b8b01cb5 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 b2b76d09a64c538c57006180103fc1841e8cfa66 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 ba3ad159aa61810bbe0acaf39578b1ebfb6f1a18 git
CNA	Linux	Linux	affected 1da177e4c3f41524e886b7f1b8a0c1fc7321cac2 a893f1757d9a4009e4a8d7ceb2312142fe29cea4 git
CNA	Linux	Linux	unaffected 6.12.83 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0.1 7.0.* semver

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/5cc0574c84aa73946ade587c41e81757b8b01cb5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ba3ad159aa61810bbe0acaf39578b1ebfb6f1a18	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/a893f1757d9a4009e4a8d7ceb2312142fe29cea4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b2b76d09a64c538c57006180103fc1841e8cfa66	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonic

CVE Program Home	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 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 and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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