



smb: server: fix use-after-free in smb2_open()

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

Summary

CVE	CVE-2026-43378
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:48 UTC
Updated	2026-05-12 14:10:27 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: smb: server: fix use-after-free in smb2_open() The opinfo

Risk And Classification

EPSS: 0.000240000 probability, percentile 0.070360000 (date 2026-05-12)

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 e1b21e6066615e7d3d3a7aa2677e415e563fd7cc gi
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 b720c84087cb547f23ce03eab93568c1769e4556 gi
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 54b48ae83de8bb06e65079d96368efe359d4909c gi
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 8f5b1a7cb009a93c48e9e334a2f59a660f9afc07 git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 190e5f808e8058640b408ccfed25440b441a718a git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 1e689a56173827669a35da7cb2a3c78ed5c53680 g
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* 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/54b48ae83de8bb06e65079d96368efe359d4909c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8f5b1a7cb009a93c48e9e334a2f59a660f9afc07	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/e1b21e6066615e7d3d3a7aa2677e415e563fd7cc	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/190e5f808e8058640b408ccfed25440b441a718a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b720c84087cb547f23ce03eab93568c1769e4556	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/1e689a56173827669a35da7cb2a3c78ed5c53680	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](#).

Free CVE JSON API cve.report/api

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