



smb: server: fix active_num_conn leak on transport allocation failure

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

Summary

CVE	CVE-2026-31711
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:21 UTC
Updated	2026-05-03 07:16:18 UTC

Description In the Linux kernel, the following vulnerability has been resolved: smb: server: fix active_num_conn leak on transport alloca

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.001150000 probability, percentile 0.298650000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 0d0d4680db22eda1eea785c47bbf66a9b33a8b16 97f8d2648ef4871e4cd335e2d769cb40054a6772 gi
CNA	Linux	Linux	affected 0d0d4680db22eda1eea785c47bbf66a9b33a8b16 295a9fc6789d1011c36ded9f0f2907bb34fa0de4 git
CNA	Linux	Linux	affected 0d0d4680db22eda1eea785c47bbf66a9b33a8b16 283027aa93380380a0994f35dde3ec95318f2654 gi
CNA	Linux	Linux	affected 0d0d4680db22eda1eea785c47bbf66a9b33a8b16 fb48185bcd946d42de7017cf27f912f8ab26acf0 git
CNA	Linux	Linux	affected 0d0d4680db22eda1eea785c47bbf66a9b33a8b16 6551300dc452ac16a855a83dbd1e74899542d3b3 c
CNA	Linux	Linux	affected 4210c3555db4b38bade92331b153e583261f05f9 git
CNA	Linux	Linux	affected d5d7847e57ac69fa99c18b363a34419bcdb5a281 git
CNA	Linux	Linux	affected 6.2
CNA	Linux	Linux	unaffected 6.2 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.84 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.25 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.2 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/97f8d2648ef4871e4cd335e2d769cb40054a6772	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6551300dc452ac16a855a83dbd1e74899542d3b3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/295a9fc6789d1011c36ded9f0f2907bb34fa0de4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/fb48185bcd946d42de7017cf27f912f8ab26acf0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/283027aa93380380a0994f35dde3ec95318f2654	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](#) 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](#)