



# smb: client: split cached\_fid bitfields to avoid shared-byte RMW races

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

## Summary

<b>CVE</b>	CVE-2026-23230
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-18 16:22:32 UTC
<b>Updated</b>	2026-04-02 15:16:24 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: smb: client: split cached\_fid bitfields to avoid shared-byte

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from nvd@nist.gov

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

**Problem Types:** NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected ebe98f1447bbccf8228335c62d86af02a0ed23f7 569fecc56bfe4df66f05734d67daef887746656b git
CNA	Linux	Linux	affected ebe98f1447bbccf8228335c62d86af02a0ed23f7 4386f6af8aaedd0c5ad6f659b40cadcc8f423828 git
CNA	Linux	Linux	affected ebe98f1447bbccf8228335c62d86af02a0ed23f7 3eaa22d688311c708b73f3c68bc6d0c8e3f0f77a git
CNA	Linux	Linux	affected ebe98f1447bbccf8228335c62d86af02a0ed23f7 c4b9edd55987384a1f201d3d07ff71e448d79c1b git
CNA	Linux	Linux	affected ebe98f1447bbccf8228335c62d86af02a0ed23f7 4cfa4c37dcbcf70866e856200ed8a2894cac578 git
CNA	Linux	Linux	affected ebe98f1447bbccf8228335c62d86af02a0ed23f7 ec306600d5ba7148c9dbf8f5a8f1f5c1a044a241 git
CNA	Linux	Linux	affected 6.1
CNA	Linux	Linux	unaffected 6.1 semver
CNA	Linux	Linux	unaffected 6.1.164 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.125 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.72 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.11 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.1 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc1 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/3eaa22d688311c708b73f3c68bc6d0c8e3f0f77a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c4b9edd55987384a1f201d3d07ff71e448d79c1b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/569fecc56bfe4df66f05734d67daef887746656b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/4386f6af8aaedd0c5ad6f659b40cadcc8f423828	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ec306600d5ba7148c9dbf8f5a8f1f5c1a044a241	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/4cfa4c37dcbcf70866e856200ed8a2894cac578	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)