



# ksmbd: set ATTR\_CTIME flags when setting mtime

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2024-57895
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-01-15 13:15:14 UTC
<b>Updated</b>	2026-04-06 14:01:29 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: ksmbd: set ATTR\_CTIME flags when setting mtime David

## 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 | CWE-noinfo Not enough information

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	ADP	DECLARED	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/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 0626e6641f6b467447c81dd7678a69c66f7746cf c7ab587bd33ce45e2aa6b6d2d36be7ef0bd16614 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 1d7ee876b8b96efc14e177a7fe8d45ac25d68849 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 52cef6ff6a4a814f4f8e357422fcb71fd2ebf75 git
CNA	Linux	Linux	affected 0626e6641f6b467447c81dd7678a69c66f7746cf 21e46a79bbe6c4e1aa73b3ed998130f2ff07b128 git
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 semver
CNA	Linux	Linux	unaffected 6.1.164 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.70 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.9 6.12.* semver
CNA	Linux	Linux	unaffected 6.13 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/52cef6ff6a4a814f4f8e357422fcb71fd2ebf75	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/21e46a79bbe6c4e1aa73b3ed998130f2ff07b128	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/1d7ee876b8b96efc14e177a7fe8d45ac25d68849	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
git.kernel.org/stable/c/c7ab587bd33ce45e2aa6b6d2d36be7ef0bd16614	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patch
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)