



# ksmbd: validate num\_aces and harden ACE walk in smb\_inherit\_dacl()

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

## Summary

<b>CVE</b>	CVE-2026-31706
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-01 14:16:20 UTC
<b>Updated</b>	2026-05-03 07:16:17 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate num\_aces and harden ACE walk in smb\_

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

**EPSS:** 0.000180000 probability, percentile 0.046600000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 063a7409b0de46d7c770b65bb0338e6fdb3b1f0a git
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 3e5360b422dd741cb315654a191fa73869a37414 gi
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 59c32abaec9cdd6164811c7e864e72f7554b82d gi
CNA	Linux	Linux	affected e2f34481b24db2fd634b5edb0a5bd0e4d38cc6e9 3e4e2ea2a781018ed5d75f969e3e5606beb66e48 gi
CNA	Linux	Linux	affected 5.15
CNA	Linux	Linux	unaffected 5.15 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/59c32abaec9cdd6164811c7e864e72f7554b82d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/3e4e2ea2a781018ed5d75f969e3e5606beb66e48	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/3e5360b422dd741cb315654a191fa73869a37414	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
git.kernel.org/stable/c/063a7409b0de46d7c770b65bb0338e6fdb3b1f0a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
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.

© 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](https://www.mitre.org)

[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)