# smb: client: fix OOBs when building SMB2_IOCTL request

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2024-50151 |
| **State** | PUBLISHED |
| **Assigner** | Linux |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2024-11-07 10:15:06 UTC |
| **Updated** | 2026-05-12 13:16:18 UTC |
| **Description** | In the Linux kernel, the following vulnerability has been resolved: smb: client: fix OOBs when building SMB2_IOCTL reques |

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-787 | CWE-787 CWE-787 Out-of-bounds Write

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | ADP | DECLARED | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/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

High

ntegrity

High

vailability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/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 e77fe73c7e38c36145825d84cfe385d400aba4fd 6f0516e |
| CNA | Linux | Linux | affected e77fe73c7e38c36145825d84cfe385d400aba4fd ed31ab |
| CNA | Linux | Linux | affected e77fe73c7e38c36145825d84cfe385d400aba4fd e07d05 |
| CNA | Linux | Linux | affected e77fe73c7e38c36145825d84cfe385d400aba4fd 2ef632b |
| CNA | Linux | Linux | affected e77fe73c7e38c36145825d84cfe385d400aba4fd b209c3 |
| CNA | Linux | Linux | affected e77fe73c7e38c36145825d84cfe385d400aba4fd fe92ddc |
| CNA | Linux | Linux | affected e77fe73c7e38c36145825d84cfe385d400aba4fd 1ab603 |
| CNA | Linux | Linux | affected 5.0 |
| CNA | Linux | Linux | unaffected 5.0 semver |
| CNA | Linux | Linux | unaffected 5.4.285 5.4.* semver |
| CNA | Linux | Linux | unaffected 5.10.229 5.10.* semver |
| CNA | Linux | Linux | unaffected 5.15.170 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.115 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.59 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.11.6 6.11.* semver |
| CNA | Linux | Linux | unaffected 6.12 * original_commit_for_fix |
| ADP | Siemens | SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem | affected * custom |

## References

| Reference | Source | Link |
|---|---|---|
| lists.debian.org/debian-lts-announce/2025/03/msg00002.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/e07d05b7f5ad9a503d9cab0afde2ab867bb65470 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/b209c3a0bc3ac172265c7fa8309e5d00654f2510 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| cert-portal.siemens.com/productcert/html/ssa-265688.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.cor |

| | | |
|---|---|---|
| git.kernel.org/stable/c/fe92ddc1c32d4474e605e3a31a4afcd0e7d765ec | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/6f0516ef1290da24b85461ed08a0938af7415e49 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/2ef632bfb888d1a14f81c1703817951e0bec5531 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/ed31aba8ce93472d9e16f5cff844ae7c94e9601d | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| lists.debian.org/debian-lts-announce/2025/01/msg00001.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/1ab60323c5201bef25f2a3dc0ccc404d9aca77f1 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

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