



tee: fix NULL pointer dereference in tee_shm_put

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-39865 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-09-19 16:15:45 UTC |
| Updated | 2026-05-12 13:17:17 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: tee: fix NULL pointer dereference in tee_shm_put tee_shm

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: CWE-476

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 c05d8f66ec3470e5212c4d08c46d6cb5738d |
| CNA | Linux | Linux | affected 492eb7afe858d60408b2da09adc78540c4d1 |
| CNA | Linux | Linux | affected dfd0743f1d9ea76931510ed150334d571fbab |
| CNA | Linux | Linux | affected dfd0743f1d9ea76931510ed150334d571fbab |
| CNA | Linux | Linux | affected dfd0743f1d9ea76931510ed150334d571fbab |
| CNA | Linux | Linux | affected dfd0743f1d9ea76931510ed150334d571fbab |
| CNA | Linux | Linux | affected dfd0743f1d9ea76931510ed150334d571fbab |
| CNA | Linux | Linux | affected dfd0743f1d9ea76931510ed150334d571fbab |
| CNA | Linux | Linux | affected 3d556a28bbfe34a80b014db49908b0f1bcb1e |
| CNA | Linux | Linux | affected b4a661b4212b8fac8853ec3b68e4a909dccc |
| CNA | Linux | Linux | affected 940e68e57ab69248fabba5889e615305789d |
| CNA | Linux | Linux | affected 5.16 |
| CNA | Linux | Linux | unaffected 5.16 semver |
| CNA | Linux | Linux | unaffected 5.10.243 5.10.* semver |
| CNA | Linux | Linux | unaffected 5.15.192 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.151 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.105 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.12.46 6.12.* semver |
| CNA | Linux | Linux | unaffected 6.16.6 6.16.* semver |
| CNA | Linux | Linux | unaffected 6.17 * original_commit_for_fix |
| ADP | Siemens | RUGGEDCOM RST2428P | affected V3.3 custom |
| ADP | Siemens | SCALANCE XC-300/XR-300/XC-400/XR-500WG/XR-500 Family | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCH328 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCM324 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCM328 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XCM332 | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRH334 24 V DC 8xFO CC | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 230 V AC 12xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 230 V AC 8xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 230V AC 2x10G 24xSFP 8xSFP | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 24 V DC 12xFO | affected V3.3 custom |

| | | | |
|-----|---------|--|----------------------|
| ADP | Siemens | SCALANCE XRM334 24 V DC 8xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 24V DC 2x10G 24xSFP 8xSFP | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 2x230 V AC 12xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 2x230 V AC 8xFO | affected V3.3 custom |
| ADP | Siemens | SCALANCE XRM334 2x230V AC 2x10G 24xSFP 8xSFP | affected V3.3 custom |
| ADP | Siemens | SIMATIC CN 4100 | affected V5.0 custom |

References

| Reference | Source | Link |
|--|--------------------------------------|---|
| lists.debian.org/debian-lts-announce/2025/10/msg00008.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| cert-portal.siemens.com/productcert/html/ssa-089022.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com |
| git.kernel.org/stable/c/4377eac565c297dfcccd2f8e9bf94ee84ff6172f | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/e4a718a3a47e89805c3be9d46a84de1949a98d5d | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| cert-portal.siemens.com/productcert/html/ssa-032379.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com |
| git.kernel.org/stable/c/add1ecc8f3ad8df22e3599c5c88d7907cc2a3079 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/25e315bc8ad363bd1194e49062f183ad4011957e | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/f266188603c34e6e234fb0dfc3185f0ba98d71b7 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| git.kernel.org/stable/c/963fca19fe34c496e04f7dd133b807b76a5434ca | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org |
| lists.debian.org/debian-lts-announce/2025/10/msg00007.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/5e07a4235bb85d9ef664411e4ff4ac34783c18ff | 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.

© 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 site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report