



# net: Fix null-ptr-deref by sock\_lock\_init\_class\_and\_name() and rmmmod.

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

## Summary

<b>CVE</b>	CVE-2025-23143
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-05-01 13:15:50 UTC
<b>Updated</b>	2026-05-12 13:16:40 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: net: Fix null-ptr-deref by sock\_lock\_init\_class\_and\_name()

## 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 ed07536ed6731775219c1df7fa26a7588753e693 83083c5fc7cf9b0f136a42f26aba60da380
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 b7489b753667bc9245958a4896c941974
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 d51e47e2ab6ef10a317d576075cf625cdf
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 feda73ad44a5cc80f6bf796bb1099a3fe71
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 905d43b8ad2436c240f844acb3ebcc7a99
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 5f7f6abd92b6c8dc8f19625ef93c3a18549
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 c11247a21aab4b50a23c8b696727d748c
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 2155802d3313d7b8365935c6b8d6edc0c
CNA	Linux	Linux	affected ed07536ed6731775219c1df7fa26a7588753e693 0bb2f7a1ad1f11d861f58e5ee5051c8974
CNA	Linux	Linux	affected 2.6.20
CNA	Linux	Linux	unaffected 2.6.20 semver
CNA	Linux	Linux	unaffected 5.4.300 5.4.* semver
CNA	Linux	Linux	unaffected 5.10.245 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.194 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.153 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.107 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.24 6.12.* semver
CNA	Linux	Linux	unaffected 6.13.12 6.13.* semver
CNA	Linux	Linux	unaffected 6.14.3 6.14.* semver
CNA	Linux	Linux	unaffected 6.15 * original_commit_for_fix
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	<a href="https://lists.debian.org">lists.debian.org</a>
git.kernel.org/stable/c/905d43b8ad2436c240f844acb3ebcc7a99b8ebf1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/d51e47e2ab6ef10a317d576075cf625cdfb96426	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/5f7f6abd92b6c8dc8f19625ef93c3a18549ede04	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/83083c5fc7cf9b0f136a42f26aba60da380f3601	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>

git.kernel.org/stable/c/2155802d3313d7b8365935c6b8d6edc0ddd7eb94	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
cert-portal.siemens.com/productcert/html/ssa-032379.html	0b142b55-0307-4c5a-b3c9-f314f3fb7c5e	<a href="https://cert-portal.siemens.com">cert-portal.siemens.com</a>
git.kernel.org/stable/c/0bb2f7a1ad1f11d861f58e5ee5051c8974ff9569	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/b7489b753667bc9245958a4896c9419743083c27	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/feda73ad44a5cc80f6bf796bb1099a3fe71576d4	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>
git.kernel.org/stable/c/c11247a21aab4b50a23c8b696727d7483de2f1e1	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>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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

**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)