



# mm/kmemleak: avoid soft lockup in \_\_kmemleak\_do\_cleanup()

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

## Summary

|                 |                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2025-39737                                                                                                           |
| State           | PUBLISHED                                                                                                                |
| Assigner        | Linux                                                                                                                    |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                             |
| Published       | 2025-09-11 17:15:35 UTC                                                                                                  |
| Updated         | 2026-05-12 13:17:08 UTC                                                                                                  |
| Description     | In the Linux kernel, the following vulnerability has been resolved: mm/kmemleak: avoid soft lockup in __kmemleak_do_clea |

## 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-401

## 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 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 9f1f4e95031f84867c5821540466d62f88 |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 1ef72a7fedc5bca70e8cc980985790de10 |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 a04de4c40aab9b338dfa989cf4aec70fd1 |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 f014c10d190b92aad366e56b445daffcd1 |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 e21a3ddd58733ce31afcb1e5dc3cb80a4  |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 8d2d22a55ffe35c38e69795468a7add1   |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 926092268efdf1ed7b55cf486356c74a9e |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 9b80430c194e4a114dc663c1025d56b4   |        |         |          |
| CNA                                         | Linux   | Linux           | affected 2abd839aa7e615f2bbc50c8ba7deb9e40d186768 d1534ae23c2b6be350c8ab060803fbf6e  |        |         |          |
| CNA                                         | Linux   | Linux           | affected 5.4                                                                         |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 5.4 semver                                                                |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 5.4.297 5.4.* semver                                                      |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 5.10.241 5.10.* semver                                                    |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 5.15.190 5.15.* semver                                                    |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 6.1.149 6.1.* semver                                                      |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 6.6.103 6.6.* semver                                                      |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 6.12.43 6.12.* semver                                                     |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 6.15.11 6.15.* semver                                                     |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 6.16.2 6.16.* semver                                                      |        |         |          |
| CNA                                         | Linux   | Linux           | unaffected 6.17 * 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/debian-lts-announce/2025/10/msg00008.html">lists.debian.org</a>     |
| git.kernel.org/stable/c/9f1f4e95031f84867c5821540466d62f88dab8ca | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/9f1f4e95031f84867c5821540466d62f88dab8ca">git.kernel.org</a> |
| git.kernel.org/stable/c/8d2d22a55ffe35c38e69795468a7add1a80e9ce  | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/8d2d22a55ffe35c38e69795468a7add1a80e9ce">git.kernel.org</a>  |
| git.kernel.org/stable/c/f014c10d190b92aad366e56b445daffcd1c075e4 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/f014c10d190b92aad366e56b445daffcd1c075e4">git.kernel.org</a> |
| git.kernel.org/stable/c/926092268efdf1ed7b55cf486356c74a9e7710d1 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/926092268efdf1ed7b55cf486356c74a9e7710d1">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/productcert/html/ssa-032379.html">cert-portal.siemens.co</a> |
| git.kernel.org/stable/c/e21a3ddd58733ce31afcb1e5dc3cb80a4b5bc29b | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/e21a3ddd58733ce31afcb1e5dc3cb80a4b5bc29b">git.kernel.org</a> |
| git.kernel.org/stable/c/9b80430c194e4a114dc663c1025d56b4f3d0153d | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/9b80430c194e4a114dc663c1025d56b4f3d0153d">git.kernel.org</a> |
| git.kernel.org/stable/c/1ef72a7fedc5bca70e8cc980985790de10d407aa | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/1ef72a7fedc5bca70e8cc980985790de10d407aa">git.kernel.org</a> |
| git.kernel.org/stable/c/a04de4c40aab9b338dfa989cf4aec70fd187eeb2 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/a04de4c40aab9b338dfa989cf4aec70fd187eeb2">git.kernel.org</a> |
| lists.debian.org/debian-lts-announce/2025/10/msg00007.html       | af854a3a-2127-422b-91ae-364da2661108 | <a href="https://lists.debian.org/debian-lts-announce/2025/10/msg00007.html">lists.debian.org</a>     |
| git.kernel.org/stable/c/d1534ae23c2b6be350c8ab060803bf6e9682adc  | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | <a href="https://git.kernel.org/stable/c/d1534ae23c2b6be350c8ab060803bf6e9682adc">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.