



mm: swap: fix race between free_swap_and_cache() and swapoff()

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2024-26960 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-05-01 06:15:12 UTC |
| Updated | 2026-05-12 12:16:28 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: mm: swap: fix race between free_swap_and_cache() and

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from ADP

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

Problem Types: CWE-362 | CWE-362 CWE-362 Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------------|-----------|-------|----------|--|
| 3.1 | ADP | DECLARED | 5.5 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 5.5 | MEDIUM | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H |

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 7c00bafee87c7bac7ed9eced7c161f8e5332cb4e d85c11 |
| CNA | Linux | Linux | affected 7c00bafee87c7bac7ed9eced7c161f8e5332cb4e 2da556 |
| CNA | Linux | Linux | affected 7c00bafee87c7bac7ed9eced7c161f8e5332cb4e 1ede7f |
| CNA | Linux | Linux | affected 7c00bafee87c7bac7ed9eced7c161f8e5332cb4e 0f98f6d |
| CNA | Linux | Linux | affected 7c00bafee87c7bac7ed9eced7c161f8e5332cb4e 3ce4c4 |
| CNA | Linux | Linux | affected 7c00bafee87c7bac7ed9eced7c161f8e5332cb4e 363d17 |
| CNA | Linux | Linux | affected 7c00bafee87c7bac7ed9eced7c161f8e5332cb4e 82b1c0 |
| CNA | Linux | Linux | affected 4.11 |
| CNA | Linux | Linux | unaffected 4.11 semver |
| CNA | Linux | Linux | unaffected 5.10.215 5.10.* semver |
| CNA | Linux | Linux | unaffected 5.15.154 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.84 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.24 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.7.12 6.7.* semver |
| CNA | Linux | Linux | unaffected 6.8.3 6.8.* semver |
| CNA | Linux | Linux | unaffected 6.9 * original_commit_for_fix |
| ADP | Linux | Linux Kernel | affected 7c00bafee87c d85c11c97ecf custom |
| ADP | Linux | Linux Kernel | affected 7c00bafee87c 2da5568ee222 custom |
| ADP | Linux | Linux Kernel | affected 7c00bafee87c 1ede7f1d7eed custom |
| ADP | Linux | Linux Kernel | affected 7c00bafee87c 0f98f6d2fb5f custom |
| ADP | Linux | Linux Kernel | affected 7c00bafee87c 3ce4c4c653e4 custom |
| ADP | Linux | Linux Kernel | affected 7c00bafee87c 363d17e7f790 custom |
| ADP | Linux | Linux Kernel | affected 7c00bafee87c 82b1c07a0af6 custom |
| ADP | Linux | Linux Kernel | unaffected 5.10.215 5.11 custom |
| ADP | Linux | Linux Kernel | unaffected 6.1.84 6.2 system |

| | | | |
|-----|---------|--|---------------------------------|
| ADP | Linux | Linux Kernel | unaffected b. 1.84 b.2 custom |
| ADP | Linux | Linux Kernel | unaffected 6.6.24 6.7 custom |
| ADP | Linux | Linux Kernel | unaffected 6.8.3 6.9 custom |
| ADP | Linux | Linux Kernel | unaffected 6.9 |
| ADP | Linux | Linux Kernel | unaffected 4.11 custom |
| ADP | Linux | Linux Kernel | affected 4.11 |
| ADP | Linux | Linux Kernel | unaffected 5.15.154 5.16 custom |
| ADP | Linux | Linux Kernel | unaffected 6.7.12 6.8 custom |
| ADP | Siemens | SIMATIC S7-1500 TM MFP - GNU/Linux Subsystem | affected * custom |

References

| Reference | Source | Link |
|---|--------------------------------------|---|
| git.kernel.org/stable/c/82b1c07a0af603e3c47b906c8e991dc96f01688e | af854a3a-2127-422b-91ae-364da2661108 | git.kernel.org |
| lists.debian.org/debian-lts-announce/2024/06/msg00017.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org |
| git.kernel.org/stable/c/0f98f6d2fb5fad00f8299b84b85b6bc1b6d7d19a | af854a3a-2127-422b-91ae-364da2661108 | git.kernel.org |
| cert-portal.siemens.com/productcert/html/ssa-265688.html | 0b142b55-0307-4c5a-b3c9-f314f3fb7c5e | cert-portal.siemens.com |
| git.kernel.org/stable/c/2da5568ee222ce0541bfe446a07998f92ed1643e | af854a3a-2127-422b-91ae-364da2661108 | git.kernel.org |
| git.kernel.org/stable/c/3ce4c4c653e4e478ecb15d3c88e690f12cbf6b39 | af854a3a-2127-422b-91ae-364da2661108 | git.kernel.org |
| git.kernel.org/stable/c/d85c11c97ecf92d47a4b29e3faca714dc1f18d0d | af854a3a-2127-422b-91ae-364da2661108 | git.kernel.org |
| git.kernel.org/stable/c/363d17e7f7907c8e27a9e86968af0eaa2301787b | af854a3a-2127-422b-91ae-364da2661108 | git.kernel.org |
| git.kernel.org/stable/c/1ede7f1d7eed1738d1b9333fd1e152ccb450b86a | af854a3a-2127-422b-91ae-364da2661108 | 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](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

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