



ext4: fix slab-use-after-free in ext4_split_extent_at()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|----------------------------------------------|
| CVE | CVE-2024-49884 |
| State | PUBLISHED |
| Assigner | Linux |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2024-10-21 18:15:11 UTC |
| Updated | 2026-05-12 19:09:03 UTC |

Description In the Linux kernel, the following vulnerability has been resolved: ext4: fix slab-use-after-free in ext4_split_extent_at() We hi

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-416

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

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 | Debian | Debian Linux | 11.0 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|-----------------------|-----------------------|------------------------------------------------------------------------------------------------|
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_393a46f60ea4f249dc9d496d4eb2d542f5e11ade git |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_448100a29395b0c8b4c42967155849fe0fbe808f git |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_e52f933598b781d291b9297e39c463536da0e185 g |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_cafcc1bd62934547c76abf46c6d0d54f135006fe git |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_a5401d4c3e2a3d25643c567d26e6de327774a2c9 g |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_8fe117790b37c84c651e2bad9efc0e7fda73c0e3 git |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_5d949ea75bb529ea6342e83465938a3b0ac51238 g |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_915ac3630488af0ca194dc63b86d99802b4f6e18 gi |
| CNA | Linux | Linux | affected dfe5080939ea4686b3414b5d970a9b26733c57a4_c26ab35702f8cd0cdc78f96aa5856bfb77be798f git |
| CNA | Linux | Linux | affected 3.18 |
| CNA | Linux | Linux | unaffected 3.18 semver |
| CNA | Linux | Linux | unaffected 4.19.323 4.19.* semver |
| CNA | Linux | Linux | unaffected 5.4.290 5.4.* semver |
| CNA | Linux | Linux | unaffected 5.10.227 5.10.* semver |
| CNA | Linux | Linux | unaffected 5.15.168 5.15.* semver |
| CNA | Linux | Linux | unaffected 6.1.113 6.1.* semver |
| CNA | Linux | Linux | unaffected 6.6.55 6.6.* semver |
| CNA | Linux | Linux | unaffected 6.10.14 6.10.* semver |
| CNA | Linux | Linux | unaffected 6.11.3 6.11.* semver |
| CNA | Linux | Linux | unaffected 6.12 * original_commit_for_fix |

References

| Reference | Source | Link | Tag |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|---------------------------------------------------------|-----|
| git.kernel.org/stable/c/8fe117790b37c84c651e2bad9efc0e7fda73c0e3 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| lists.debian.org/debian-lts-announce/2025/03/msg00002.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org | Mai |
| git.kernel.org/stable/c/393a46f60ea4f249dc9d496d4eb2d542f5e11ade | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| git.kernel.org/stable/c/c26ab35702f8cd0cdc78f96aa5856bfb77be798f | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| git.kernel.org/stable/c/448100a29395b0c8b4c42967155849fe0fbe808f | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| git.kernel.org/stable/c/cafcc1bd62934547c76abf46c6d0d54f135006fe | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |

| | | | |
|------------------------------------------------------------------|--------------------------------------|---------------------------------------------------------|-----|
| git.kernel.org/stable/c/5d949ea75bb529ea6342e83465938a3b0ac51238 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| git.kernel.org/stable/c/915ac3630488af0ca194dc63b86d99802b4f6e18 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| lists.debian.org/debian-lts-announce/2025/01/msg00001.html | af854a3a-2127-422b-91ae-364da2661108 | lists.debian.org | Bro |
| git.kernel.org/stable/c/e52f933598b781d291b9297e39c463536da0e185 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| git.kernel.org/stable/c/a5401d4c3e2a3d25643c567d26e6de327774a2c9 | 416baaa9-dc9f-4396-8d5f-8c081fb06d67 | git.kernel.org | Pat |
| CVE Program record | CVE.ORG | www.cve.org | can |
| NVD vulnerability detail | NVD | nvd.nist.gov | can |

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/licenses).

Free CVE JSON API cve.report/api

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