



# ext4: fix double brelse() the buffer of the extents path

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2024-49882
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-10-21 18:15:10 UTC
<b>Updated</b>	2026-05-12 19:08:45 UTC
<b>Description</b>	In the Linux kernel, the following vulnerability has been resolved: ext4: fix double brelse() the buffer of the extents path In e

## 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-415

## 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	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 d4574bda63906bf69660e001470bfe1a0ac524ae git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 f9fd47c9d9548f9e47fa60098eab99dde175401d git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 b6c29c8f3d7cb67b505f3b2f6c242d52298d1f2e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 32bbb59e3f18facd7201bef110010bf35819b8c3 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 78bbc3d15b6f443acb26e94418c445bac940d414 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 68a69cf60660c73990c1875f94a5551600b04775 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 7633407ca4ab8be2916ab214eb44cceb6a50e1a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 230ee0535d01478bad9a3037292043f39b9be10b git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ecb94f5fdf4b72547fca022421a9dca1672bddd4 dcaa6c31134c0f515600111c38ed7750003e1b9c git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.7
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.7 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 4.19.323 4.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.4.285 5.4.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.227 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.168 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.113 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.55 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.10.14 6.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.11.3 6.11.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12 * original_commit_for_fix

## References

Reference	Source	Link	Tag
lists.debian.org/debian-lts-announce/2025/03/msg00002.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>	Mail
git.kernel.org/stable/c/7633407ca4ab8be2916ab214eb44cceb6a50e1a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/68a69cf60660c73990c1875f94a5551600b04775	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/b6c29c8f3d7cb67b505f3b2f6c242d52298d1f2e	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/d4574bda63906bf69660e001470bfe1a0ac524ae	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/78bbc3d15b6f443acb26e94418c445bac940d414	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc

git.kernel.org/stable/c/f9fd47c9d9548f9e47fa60098eab99dde175401d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/230ee0535d01478bad9a3037292043f39b9be10b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
git.kernel.org/stable/c/32bbb59e3f18facd7201bef110010bf35819b8c3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
lists.debian.org/debian-lts-announce/2025/01/msg00001.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>	Mail
git.kernel.org/stable/c/dcaa6c31134c0f515600111c38ed7750003e1b9c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	Patc
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canc
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canc

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)