



# erofs: fix UAF issue for file-backed mounts w/ directio option

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

## Summary

<b>CVE</b>	CVE-2026-23224
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-02-18 16:22:32 UTC
<b>Updated</b>	2026-04-02 15:16:23 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: erofs: fix UAF issue for file-backed mounts w/ directio opti

## 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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

## 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	Linux	Linux Kernel	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected fb176750266a3d7f42ebdcf28e8ba40350b27847 ae385826840a3c8e09bf38cac90adcd690716f57 git
CNA	Linux	Linux	affected fb176750266a3d7f42ebdcf28e8ba40350b27847 d741534302f71c511eb0bb670b92eaa7df4a0aec git
CNA	Linux	Linux	affected fb176750266a3d7f42ebdcf28e8ba40350b27847 b2ee5e4d5446babd23ff7beb4e636be0fb3ea5aa git
CNA	Linux	Linux	affected fb176750266a3d7f42ebdcf28e8ba40350b27847 1caf50ce4af096d0280d59a31abdd85703cd995c git
CNA	Linux	Linux	affected 6.12
CNA	Linux	Linux	unaffected 6.12 semver
CNA	Linux	Linux	unaffected 6.12.72 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.11 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.1 6.19.* semver
CNA	Linux	Linux	unaffected 7.0-rc1 * original_commit_for_fix

### References

Reference	Source	Link	Tags
git.kernel.org/stable/c/ae385826840a3c8e09bf38cac90adcd690716f57	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/d741534302f71c511eb0bb670b92eaa7df4a0aec	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/1caf50ce4af096d0280d59a31abdd85703cd995c	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/b2ee5e4d5446babd23ff7beb4e636be0fb3ea5aa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**