



mm: call ->free_folio() directly in folio_unmap_invalidate()

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary

CVE	CVE-2026-31589
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:34 UTC
Updated	2026-04-28 20:40:06 UTC

Description

In the Linux kernel, the following vulnerability has been resolved: mm: call ->free_folio() directly in folio_unmap_invalidate()

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000170000 probability, percentile 0.040590000 (date 2026-04-27)

Problem Types: CWE-416

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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 fb7d3bc4149395c1ae99029c852eab6c28fc3c88 b667df39d98a7a24be7c2a40ff0863dac1ad2cd7 git
CNA	Linux	Linux	affected fb7d3bc4149395c1ae99029c852eab6c28fc3c88 c330e65ea59c4805d6ab6757c4ddfe8c63acef31 git
CNA	Linux	Linux	affected fb7d3bc4149395c1ae99029c852eab6c28fc3c88 615d9bb2ccad42f9e21d837431e401db2e471195 git
CNA	Linux	Linux	affected 6.14
CNA	Linux	Linux	unaffected 6.14 semver
CNA	Linux	Linux	unaffected 6.19.14 6.19.* semver
CNA	Linux	Linux	unaffected 7.0.1 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References			
Reference	Source	Link	Tags
git.kernel.org/stable/c/615d9bb2ccad42f9e21d837431e401db2e471195	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c330e65ea59c4805d6ab6757c4ddfe8c63acef31	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/b667df39d98a7a24be7c2a40ff0863dac1ad2cd7	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.

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](#).

Free CVE JSON API cve.report/api

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