



fuse: reject oversized dirents in page cache

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

Summary

CVE	CVE-2026-31694
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:19 UTC
Updated	2026-05-03 07:16:16 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: fuse: reject oversized dirents in page cache fuse_add_dir

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000180000 probability, percentile 0.048520000 (date 2026-05-02)

Version	Source	Type	Score	Severity	Vector
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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 69e34551152a286f827d54dcb5700da6aeaac1fb d23ad78bfd205eac26766e38ba7d79f279131098 git
CNA	Linux	Linux	affected 69e34551152a286f827d54dcb5700da6aeaac1fb 45c05af36311624c1148123caeb011312495d86b gi
CNA	Linux	Linux	affected 69e34551152a286f827d54dcb5700da6aeaac1fb 7de93abfaae1b2dc94da8a07a36421bd073f1d8f git
CNA	Linux	Linux	affected 69e34551152a286f827d54dcb5700da6aeaac1fb 474ce83c96a55f2eeb14dee2be375eeadfdacdf5 git
CNA	Linux	Linux	affected 69e34551152a286f827d54dcb5700da6aeaac1fb 51a8de6c50bf947c8f534cd73da4c8f0a13e7bed git
CNA	Linux	Linux	affected 4.20
CNA	Linux	Linux	unaffected 4.20 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.84 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.25 6.18.* semver
CNA	Linux	Linux	unaffected 7.0.2 7.0.* semver
CNA	Linux	Linux	unaffected 7.1-rc1 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/45c05af36311624c1148123caeb011312495d86b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/51a8de6c50bf947c8f534cd73da4c8f0a13e7bed	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/7de93abfaae1b2dc94da8a07a36421bd073f1d8f	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/474ce83c96a55f2eeb14dee2be375eeadfdacdf5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/d23ad78bfd205eac26766e38ba7d79f279131098	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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.

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