ocfs2: fix use-after-free in ocfs2_fault() when VM_FAULT_RETRY

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-31597
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 15:16:37 UTC
Updated	2026-04-29 14:15:58 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix use-after-free in ocfs2_fault() when VM_FAULT_

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 0.048130000 (date 2026-04-27)

Problem Types: CWE-416

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

ntegrity

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 614a9e849ca6ea24843795251cb30af525d5336b 6f072daefcab1d84ce37c073645615f63be91006 git
CNA	Linux	Linux	affected 614a9e849ca6ea24843795251cb30af525d5336b 4cf2768a0291a0cdd0dae801ea0eafa3878a349d gi
CNA	Linux	Linux	affected 614a9e849ca6ea24843795251cb30af525d5336b d45ff441b416d4aa1af72b1db23d959601c04da2 git
CNA	Linux	Linux	affected 614a9e849ca6ea24843795251cb30af525d5336b 76a602fdbb78dd05b2da06f74a988cebc97e82d0 gi
CNA	Linux	Linux	affected 614a9e849ca6ea24843795251cb30af525d5336b 925bf22c1b823e231b1baea761fe8a1512e442f2 git
CNA	Linux	Linux	affected 614a9e849ca6ea24843795251cb30af525d5336b 7de554cabf160e331e4442e2a9ad874ca9875921 g
CNA	Linux	Linux	affected 2.6.39
CNA	Linux	Linux	unaffected 2.6.39 semver
CNA	Linux	Linux	unaffected 6.6.136 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.83 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.24 6.18.* 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/d45ff441b416d4aa1af72b1db23d959601c04da2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/925bf22c1b823e231b1baea761fe8a1512e442f2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/4cf2768a0291a0cdd0dae801ea0eafa3878a349d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/76a602fdbb78dd05b2da06f74a988cebc97e82d0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/7de554cabf160e331e4442e2a9ad874ca9875921	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/6f072daefcab1d84ce37c073645615f63be91006	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canonic

NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

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