f2fs: fix UAF caused by decrementing sbi->nr_pages[] in f2fs_write_end_io()

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

Summary

CVE	CVE-2026-31715
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:21 UTC
Updated	2026-05-07 06:16:04 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix UAF caused by decrementing sbi->nr_pages[] in f

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

EPSS: 0.000170000 probability, percentile 0.040610000 (date 2026-05-05)

Problem Types: CWE-416

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 50fa53eccf9f911a5b435248a2b0bd484fd82e5e 7be222de96c0f9eee6e65eeb017ef855ee185cfa git
CNA	Linux	Linux	affected 50fa53eccf9f911a5b435248a2b0bd484fd82e5e 963d2e24d9d92a31e6773b0f642214f10013ebf7 git
CNA	Linux	Linux	affected 50fa53eccf9f911a5b435248a2b0bd484fd82e5e 188bb65f247a7a7c62f287c9a263aee3cad96fa5 git
CNA	Linux	Linux	affected 50fa53eccf9f911a5b435248a2b0bd484fd82e5e 2d9c4a4ed4eef1f82c5b16b037aee8bad819fd53 git
CNA	Linux	Linux	affected 4.19
CNA	Linux	Linux	unaffected 4.19 semver
CNA	Linux	Linux	unaffected 6.12.86 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/963d2e24d9d92a31e6773b0f642214f10013ebf7	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/2d9c4a4ed4eef1f82c5b16b037aee8bad819fd53	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/188bb65f247a7a7c62f287c9a263aee3cad96fa5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/7be222de96c0f9eee6e65eeb017ef855ee185cfa	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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