f2fs: fix use-after-free of sbi in f2fs_compress_write_end_io()

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

Summary

CVE	CVE-2026-31702
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-01 14:16:20 UTC
Updated	2026-05-06 18:44:52 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix use-after-free of sbi in f2fs_compress_write_end_i

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: 0.000180000 probability, percentile 0.048290000 (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 4c8ff7095bef64fc47e996a938f7d57f9e077da3 ef57cd3329b40c739b9a2e1a8a21ecc4171c6280 git
CNA	Linux	Linux	affected 4c8ff7095bef64fc47e996a938f7d57f9e077da3 f5154cf3ce1c8193f0c1891d3769f62740cfe6fe git
CNA	Linux	Linux	affected 4c8ff7095bef64fc47e996a938f7d57f9e077da3 c76cf339b87975ae5b2c06d2d774d5667d25a12a git
CNA	Linux	Linux	affected 4c8ff7095bef64fc47e996a938f7d57f9e077da3 2c97dcb6147c8f7f25c629b93be1e69617de5d4a git
CNA	Linux	Linux	affected 4c8ff7095bef64fc47e996a938f7d57f9e077da3 39d4ee19c1e7d753dd655aebee632271b171f43a git
CNA	Linux	Linux	affected 5.6
CNA	Linux	Linux	unaffected 5.6 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/2c97dcb6147c8f7f25c629b93be1e69617de5d4a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/39d4ee19c1e7d753dd655aebee632271b171f43a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/ef57cd3329b40c739b9a2e1a8a21ecc4171c6280	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/c76cf339b87975ae5b2c06d2d774d5667d25a12a	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/f5154cf3ce1c8193f0c1891d3769f62740cfe6fe	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.

Free CVE JSON API cve.report/api

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