scsi: core: Wake up the error handler when final completions race against each other

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

Summary

CVE	CVE-2026-23110
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-04 17:16:21 UTC
Updated	2026-04-18 09:16:13 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Wake up the error handler when final completic

Risk And Classification

Primary CVSS: v3.1 4.7 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-362

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/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 6eb045e092efefafc6687409a6fa6d1dabf0fb69 48cbc304c5ea796421f7d10b7798fa581970c080 git
CNA	Linux	Linux	affected 6eb045e092efefafc6687409a6fa6d1dabf0fb69 6d9a367be356101963c249ebf10ea10b32886607 git
CNA	Linux	Linux	affected 6eb045e092efefafc6687409a6fa6d1dabf0fb69 9fdc6f28d5e81350ab1d2cac8389062bd09e61e1 git
CNA	Linux	Linux	affected 6eb045e092efefafc6687409a6fa6d1dabf0fb69 64ae21b9c4f0c7e60cf47a53fa7ab68852079ef0 git
CNA	Linux	Linux	affected 6eb045e092efefafc6687409a6fa6d1dabf0fb69 219f009ebfd1ef3970888ee9eef4c8a06357f862 git
CNA	Linux	Linux	affected 6eb045e092efefafc6687409a6fa6d1dabf0fb69 fe2f8ad6f0999db3b318359a01ee0108c703a8c3 git
CNA	Linux	Linux	affected 5.5
CNA	Linux	Linux	unaffected 5.5 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 6.1.162 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.122 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.68 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.8 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/fe2f8ad6f0999db3b318359a01ee0108c703a8c3	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/219f009ebfd1ef3970888ee9eef4c8a06357f862	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/6d9a367be356101963c249ebf10ea10b32886607	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/48cbc304c5ea796421f7d10b7798fa581970c080	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/9fdc6f28d5e81350ab1d2cac8389062bd09e61e1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/64ae21b9c4f0c7e60cf47a53fa7ab68852079ef0	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.