libceph: reset sparse-read state in osd_fault()

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2026-23136
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-14 16:15:53 UTC
Updated	2026-04-03 14:16:24 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: libceph: reset sparse-read state in osd_fault() When a fau

Risk And Classification

Primary CVSS: v3.1 5.5 MEDIUM from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:L/AC:L/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 f628d799972799023d32c2542bb2639eb8c4f84e 90a60fe61908afa0eaf7f8fcf1421b9b50e5f7ff git
CNA	Linux	Linux	affected f628d799972799023d32c2542bb2639eb8c4f84e e94075e950a6598e710b9f7dffea5aa388f40313 git
CNA	Linux	Linux	affected f628d799972799023d32c2542bb2639eb8c4f84e 10b7c72810364226f7b27916ea3e2a4f870bc04b git
CNA	Linux	Linux	affected f628d799972799023d32c2542bb2639eb8c4f84e 11194b416ef95012c2cfe5f546d71af07b639e93 git
CNA	Linux	Linux	affected 6.6
CNA	Linux	Linux	unaffected 6.6 semver
CNA	Linux	Linux	unaffected 6.6.121 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.66 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.6 6.18.* semver
CNA	Linux	Linux	unaffected 6.19 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/11194b416ef95012c2cfe5f546d71af07b639e93	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/90a60fe61908afa0eaf7f8fcf1421b9b50e5f7ff	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/10b7c72810364226f7b27916ea3e2a4f870bc04b	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
git.kernel.org/stable/c/e94075e950a6598e710b9f7dffea5aa388f40313	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	Patch
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.

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