libceph: Fix potential out-of-bounds access in ceph_handle_auth_reply()

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

Summary

CVE	CVE-2026-43407
State	PUBLISHED
Assigner	Linux
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-08 15:16:52 UTC
Updated	2026-05-11 08:16:13 UTC
Description	In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential out-of-bounds access in ceph_handl

Risk And Classification

Primary CVSS: v3.1 9.1 CRITICAL from 416baaa9-dc9f-4396-8d5f-8c081fb06d67

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

EPSS: 0.000240000 probability, percentile 0.070400000 (date 2026-05-10)

Version	Source	Type	Score	Severity	Vector
3.1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
3.1	CNA	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc ea080b21092590122c3f971cf588932cdbf47847 git
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc edc678e5cd11730a2834b43071d8923f05bc334d g
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc 6cee34d6669fe176b4259131adb1a145c939b472 g
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc 8bb87547e92dcf0928ed763c60e0ac8d733c3656 gi
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc ed024d2f4c79c0eb2464df0fb640610ac301f9a0 git
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc f9da5c1bbac5c8e33259fe00ed7347438fffa969 git
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc 9f9e2297f45fc2d2524eb104c289d69ddef95665 git
CNA	Linux	Linux	affected 4e7a5dcd1bbab6560fbc8ada29a840e7a20ed7bc b282c43ed156ae15ea76748fc15cd5c39dc9ab72 gi
CNA	Linux	Linux	affected 2.6.34
CNA	Linux	Linux	unaffected 2.6.34 semver
CNA	Linux	Linux	unaffected 5.10.253 5.10.* semver
CNA	Linux	Linux	unaffected 5.15.203 5.15.* semver
CNA	Linux	Linux	unaffected 6.1.167 6.1.* semver
CNA	Linux	Linux	unaffected 6.6.130 6.6.* semver
CNA	Linux	Linux	unaffected 6.12.78 6.12.* semver
CNA	Linux	Linux	unaffected 6.18.19 6.18.* semver
CNA	Linux	Linux	unaffected 6.19.9 6.19.* semver
CNA	Linux	Linux	unaffected 7.0 * original_commit_for_fix

References

Reference	Source	Link	Tags
git.kernel.org/stable/c/9f9e2297f45fc2d2524eb104c289d69ddef95665	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/edc678e5cd11730a2834b43071d8923f05bc334d	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/8bb87547e92dcf0928ed763c60e0ac8d733c3656	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/f9da5c1bbac5c8e33259fe00ed7347438fffa969	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/6cee34d6669fe176b4259131adb1a145c939b472	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/b282c43ed156ae15ea76748fc15cd5c39dc9ab72	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/ed024d2f4c79c0eb2464df0fb640610ac301f9a0	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	

git.kernel.org/stable/c/ea080b2109259012 2c3f971cf588932cdbf47847	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
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.