



libceph: prevent potential out-of-bounds reads in process_message_header()

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-43406
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: prevent potential out-of-bounds reads in process

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 cd1a677cad994021b19665ed476aea63f5d54f31 76ccf21a12c5f6d6790bc32c7da82446d877b2f4 git
CNA	Linux	Linux	affected cd1a677cad994021b19665ed476aea63f5d54f31 75582aaa580c11aed4c7731cad6b068b700e7efb gi
CNA	Linux	Linux	affected cd1a677cad994021b19665ed476aea63f5d54f31 50156622eb0888e62541d715a98584480a1bc7cb g
CNA	Linux	Linux	affected cd1a677cad994021b19665ed476aea63f5d54f31 dbd857a9e1e33ea71eaf3e211877027e533770d1 gi
CNA	Linux	Linux	affected cd1a677cad994021b19665ed476aea63f5d54f31 69fe5af33fa3806f398d21c081d73c66e5523bc2 git
CNA	Linux	Linux	affected cd1a677cad994021b19665ed476aea63f5d54f31 035867ae6f18df0aeedb2a57a5b74091bd4e3fe8 git
CNA	Linux	Linux	affected cd1a677cad994021b19665ed476aea63f5d54f31 69fb5d91bba44ecf7eb80530b85fa4fb028921d5 git
CNA	Linux	Linux	affected 5.11
CNA	Linux	Linux	unaffected 5.11 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/50156622eb0888e62541d715a98584480a1bc7cb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/75582aaa580c11aed4c7731cad6b068b700e7efb	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/69fb5d91bba44ecf7eb80530b85fa4fb028921d5	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/69fe5af33fa3806f398d21c081d73c66e5523bc2	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/dbd857a9e1e33ea71eaf3e211877027e533770d1	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/035867ae6f18df0aeedb2a57a5b74091bd4e3fe8	416baaa9-dc9f-4396-8d5f-8c081fb06d67	git.kernel.org	
git.kernel.org/stable/c/76ccf21a12c5f6d6790bc32c7da82446d877b2f4	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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)