



# ceph: supply snapshot context in ceph\_zero\_partial\_object()

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

## Summary

<b>CVE</b>	CVE-2026-43273
<b>State</b>	PUBLISHED
<b>Assigner</b>	Linux
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-06 12:16:48 UTC
<b>Updated</b>	2026-05-06 13:07:51 UTC

**Description** In the Linux kernel, the following vulnerability has been resolved: ceph: supply snapshot context in ceph\_zero\_partial\_objec

## Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 36673344b41c31fb502dd0d0113cec1aa96f581e git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 5788b742007f53406049bef917833a71ddd43f60 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 757873abfc8ea38592582180aed0f57f0f0cb07a git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 9efa154609cdb658f51c7d76b30a09f7e6485250 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 531a76c5a2e44264cee8a70121e63eb28c1ba728 gi
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 69e59a87bab0ea31ab2a584fc65e12dafacf8953 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 4097e70fc543cca72982854108a32f6ae924e727 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected ad7a60de882aca31afb58721db166f7e77afcd92 f16bd3fa74a2084ee7e16a8a2be7e7399b970907 git
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	affected 3.12
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 3.12 semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.10.252 5.10.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 5.15.202 5.15.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.1.165 6.1.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.6.128 6.6.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.12.75 6.12.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.18.16 6.18.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 6.19.6 6.19.* semver
CNA	<a href="#">Linux</a>	<a href="#">Linux</a>	unaffected 7.0 * original_commit_for_fix

## References

Reference	Source	Link	Tags
<a href="https://git.kernel.org/stable/c/5788b742007f53406049bef917833a71ddd43f60">git.kernel.org/stable/c/5788b742007f53406049bef917833a71ddd43f60</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/757873abfc8ea38592582180aed0f57f0f0cb07a">git.kernel.org/stable/c/757873abfc8ea38592582180aed0f57f0f0cb07a</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/36673344b41c31fb502dd0d0113cec1aa96f581e">git.kernel.org/stable/c/36673344b41c31fb502dd0d0113cec1aa96f581e</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/f16bd3fa74a2084ee7e16a8a2be7e7399b970907">git.kernel.org/stable/c/f16bd3fa74a2084ee7e16a8a2be7e7399b970907</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/531a76c5a2e44264cee8a70121e63eb28c1ba728">git.kernel.org/stable/c/531a76c5a2e44264cee8a70121e63eb28c1ba728</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/69e59a87bab0ea31ab2a584fc65e12dafac8953">git.kernel.org/stable/c/69e59a87bab0ea31ab2a584fc65e12dafac8953</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/9efa154609cdb658f51c7d76b30a09f7e6485250">git.kernel.org/stable/c/9efa154609cdb658f51c7d76b30a09f7e6485250</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
<a href="https://git.kernel.org/stable/c/4097e70fc543cca72982854108a32f6ae924e727">git.kernel.org/stable/c/4097e70fc543cca72982854108a32f6ae924e727</a>	416baaa9-dc9f-4396-8d5f-8c081fb06d67	<a href="https://git.kernel.org">git.kernel.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)