



CVE-2020-10736

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

Summary

CVE	CVE-2020-10736
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-22 18:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	An authorization bypass vulnerability was found in Ceph versions 15.2.0 before 15.2.2, where the ceph-mon and ceph-mgr

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Ceph	All	All	All	All
Application	Linuxfoundation	Ceph	All	All	All	All

References

Reference	Source	Link
Ceph v15.2.2 Octopus released - Ceph	MISC	ceph.io
1833025 – (CVE-2020-10736) CVE-2020-10736 ceph: authorization bypass in monitor and manager daemons	CONFIRM	bugzilla.redhat.
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501531](#) Alpine Linux Security Update for ceph

[502825](#) Alpine Linux Security Update for ceph16

[505715](#) Alpine Linux Security Update for ceph16

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)