



CVE-2020-25660

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

Summary

CVE	CVE-2020-25660
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-23 22:15:00 UTC
Updated	2023-11-07 03:20:00 UTC
Description	A flaw was found in the Cephx authentication protocol in versions before 15.2.6 and before 14.2.14, where it does not verify

Risk And Classification

Problem Types: CWE-294

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Redhat	Ceph	All	All	All	All
Application	Redhat	Ceph	All	All	All	All
Application	Redhat	Ceph	All	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	4.0	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	4.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora 33 Update: ceph-15.2.7-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	Mailing
Ceph v14.2.14 Nautilus released - Ceph	MISC	ceph.io	Relea
1890354 - (CVE-2020-25660) CVE-2020-25660 ceph: CEPHX_V2 replay attack protection lost	MISC	bugzilla.redhat.com	Issue

Ceph v15.2.6 Octopus released - Ceph	MISC	ceph.io	Relea:
Ceph: Multiple vulnerabilities (GLSA 202105-39) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 33 Update: ceph-15.2.7-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[239757](#) Red Hat Update for red hat ceph storage 4.2 (RHSA-2021:0081)

[500843](#) Alpine Linux Security Update for ceph

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

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

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

[710075](#) Gentoo Linux Ceph Multiple vulnerabilities (GLSA 202105-39)

[750541](#) OpenSUSE Security Update for ceph (openSUSE-SU-2020:2082-1)

[750551](#) OpenSUSE Security Update for ceph (openSUSE-SU-2020:2057-1)

© [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