



CVE-2020-27781

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

Summary

CVE	CVE-2020-27781
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-18 21:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	User credentials can be manipulated and stolen by Native CephFS consumers of OpenStack Manila, resulting in potential p

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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 Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	3.0	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	3.0	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
Application	Redhat	Openstack Platform	13.0	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All

References

Reference

[SECURITY] [DLA 3629-1] ceph security update

[SECURITY] Fedora 33 Update: ceph-15.2.8-1.fc33 - package-announce - Fedora Mailing-Lists

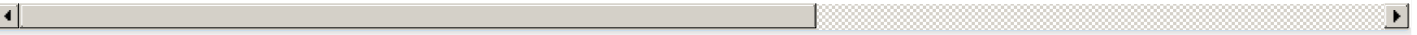
[SECURITY] Fedora 33 Update: ceph-15.2.8-1.fc33 - package-announce - Fedora Mailing-Lists

Ceph: Multiple vulnerabilities (GLSA 202105-39) — Gentoo security

1900109 – (CVE-2020-27781) CVE-2020-27781 Ceph: User credentials can be manipulated and stolen by Native CephFS consumers of Ope

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[198423](#) Ubuntu Security Notification for Ceph vulnerabilities (USN-4998-1)

[198554](#) Ubuntu Security Notification for Ceph Vulnerabilities (USN-5128-1)

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

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

[501532](#) Alpine Linux Security Update for ceph

[502826](#) Alpine Linux Security Update for ceph16

[6000278](#) Debian Security Update for ceph (DLA 3629-1)

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

[750422](#) OpenSUSE Security Update for ceph (openSUSE-SU-2021:0079-1)

[750466](#) OpenSUSE Security Update for ceph (openSUSE-SU-2020:2327-1)

© [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](#)