



CVE-2020-25678

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

Summary

CVE	CVE-2020-25678
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-08 18:15:00 UTC
Updated	2023-10-23 19:15:00 UTC
Description	A flaw was found in ceph in versions prior to 16.y.z where ceph stores mgr module passwords in clear text. This can be fou

Risk And Classification

Problem Types: CWE-312

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	4.0	All	All	All
Application	Redhat	Ceph Storage	4.0	All	All	All

References

Reference	Source	Link
Bug #37503: Audit log: mgr module passwords set on CLI written as plaintext in log files - Ceph - Ceph	MISC	tracker.ceph.com
[SECURITY] [DLA 3629-1] ceph security update	MISC	lists.debian.org
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.cor
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.cor
1892109 – (CVE-2020-25678) CVE-2020-25678 ceph: mgr modules' passwords are in clear text in mgr logs	MISC	bugzilla.redhat.co
Ceph: Multiple vulnerabilities (GLSA 202105-39) — Gentoo security	GENTOO	security.gentoo.or
[SECURITY] Fedora 33 Update: ceph-15.2.9-1.fc33 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject
[SECURITY] Fedora 33 Update: ceph-15.2.9-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[174881](#) SUSE Enterprise Linux Security Update for ceph (SUSE-SU-2021:1108-1)

[174975](#) SUSE Enterprise Linux Security Update for ceph (SUSE-SU-2021:1473-1)

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

[239270](#) Red Hat Update for Red Hat Ceph Storage (RHSA-2021:1452)

[281589](#) Fedora Security Update for ceph (FEDORA-2021-93ff9e9103)

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

[670358](#) EulerOS Security Update for ceph (EulerOS-SA-2021-1866)

[670860](#) EulerOS Security Update for ceph (EulerOS-SA-2021-1866)

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

[750271](#) OpenSUSE Security Update for ceph (openSUSE-SU-2021:0544-1)

© [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](#)