



CVE-2020-1716

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

Summary

CVE	CVE-2020-1716
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-28 13:15:00 UTC
Updated	2021-06-10 15:27:00 UTC
Description	A flaw was found in the ceph-ansible playbook where it contained hardcoded passwords that were being used as default pa

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ceph	Ceph-ansible	All	All	All	All

References

Reference	Source	Link
1795592 – (CVE-2020-1716) CVE-2020-1716 ceph-ansible: hard coded credential in ceph-ansible playbook	MISC	bugzilla.redhat.co
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

[960763](#) Rocky Linux Security Update for Rocky (RLSA-2020:2231)

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](#)