



CVE-2020-8566

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

Summary

CVE	CVE-2020-8566
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-07 22:15:00 UTC
Updated	2021-03-29 19:30:00 UTC
Description	In Kubernetes clusters using Ceph RBD as a storage provisioner, with logging level of at least 4, Ceph RBD admin secrets

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	All	All	All	All

References

Reference	Source
[Security Advisory] Multiple secret leaks when verbose logging is enabled	MLIST
December 2020 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM
CVE-2020-8566: Ceph RBD adminSecrets exposed in logs when loglevel >= 4 · Issue #95624 · kubernetes/kubernetes · GitHub	CONFIRM
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Kaizhe Huang (derek0405)

Legacy QID Mappings

[377847](#) Kubernetes Ceph RBD Admin Secrets exposed Vulnerability

[770064](#) Red Hat OpenShift Container Platform 4.7.0 Packages and Security Update (RHSA-2020:5634)

[900232](#) CBL-Mariner Linux Security Update for kubernetes 1.18.10

© [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](#)