



CVE-2020-8563

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

Summary

CVE	CVE-2020-8563
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 19:31:00 UTC
Description	In Kubernetes clusters using VSphere as a cloud provider, with a logging level set to 4 or above, VSphere cloud credentials

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	MITRE
December 2020 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	CVE
CVE-2020-8563: Secret leaks in kube-controller-manager when using vSphere provider · Issue #95621 · kubernetes/kubernetes · GitHub	CVE
CVE Program record	CVE
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Kaizhe Huang (derek0405)

Legacy QID Mappings

[377851](#) Kubernetes kube-Controller-Manager Secret Leaks Vulnerability

770042 Red Hat OpenShift Container Platform 4.6.8 Security and Packages Update (RHSA-2020:5260)
900229 CBL-Mariner Linux Security Update for kubernetes 1.18.17
900230 CBL-Mariner Linux Security Update for kubernetes-1.18.14 1.18.14
900231 CBL-Mariner Linux Security Update for kubernetes-1.18.17 1.18.17
903276 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (3652)
903290 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.18.17 (4276)
903496 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.18.14 (4274)
903556 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.18.19 (5469)
903615 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.18.17 (5465)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)