



CVE-2020-8564

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-8564
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 a logging level of at least 4, processing a malformed docker config file will result in the content

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	S
[Security Advisory] Multiple secret leaks when verbose logging is enabled	M
December 2020 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	C
CVE-2020-8564: Docker config secrets leaked when file is malformed and log level >= 4 · Issue #95622 · kubernetes/kubernetes · GitHub	C
CVE Program record	C
NVD vulnerability detail	N

Vendor Comments And Credit

Discovery Credit

LEGACY: Nikolaos Moraitis (Red Hat)

Legacy QID Mappings

[239607](#) Red Hat Update for OpenShift Container Platform 3.11.z (RHSA-2021:3193)

377852	Kubernetes Docker Config Secrets Leaked Vulnerability
770039	Red Hat OpenShift Container Platform 4.6.1 Package Security Update (RHSA-2020:4297)
770076	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:0172)
770116	Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-0172)
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](#)