



CVE-2020-8565

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

Summary

CVE	CVE-2020-8565
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-07 22:15:00 UTC
Updated	2020-12-08 19:51:00 UTC
Description	In Kubernetes, if the logging level is set to at least 9, authorization and bearer tokens will be written to log files. This can occur

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
Application	Kubernetes	Kubernetes	All	All	All	All

References

Reference
[Security Advisory] Multiple secret leaks when verbose logging is enabled
CVE-2020-8565: Incomplete fix for CVE-2019-11250 allows for token leak in logs when logLevel >= 9 · Issue #95623 · kubernetes/kubernetes
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit
LEGACY: Patrick Rhomberg (purelyapplied)

Legacy QID Mappings

[377848](#) Kubernetes Token Leak Logs Vulnerability

900233 CBL-Mariner Linux Security Update for kubernetes 1.17.13
903419 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (3697)

© [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](#)