



CVE-2019-11250

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

Summary

CVE	CVE-2019-11250
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-29 01:15:00 UTC
Updated	2020-10-16 09:15:00 UTC
Description	The Kubernetes client-go library logs request headers at verbosity levels of 7 or higher. This can disclose credentials to unauthorized users.

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	1.15.3	-	All	All
Application	Kubernetes	Kubernetes	1.15.4	beta0	All	All
Application	Kubernetes	Kubernetes	1.16.0	alpha1	All	All
Application	Kubernetes	Kubernetes	1.16.0	alpha2	All	All
Application	Kubernetes	Kubernetes	1.16.0	alpha3	All	All
Application	Kubernetes	Kubernetes	1.16.0	beta1	All	All
Application	Kubernetes	Kubernetes	1.16.0	beta2	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.15.3	-	All	All
Application	Kubernetes	Kubernetes	1.15.4	beta0	All	All
Application	Kubernetes	Kubernetes	1.16.0	alpha1	All	All
Application	Kubernetes	Kubernetes	1.16.0	alpha2	All	All
Application	Kubernetes	Kubernetes	1.16.0	alpha3	All	All
Application	Kubernetes	Kubernetes	1.16.0	beta1	All	All
Application	Kubernetes	Kubernetes	1.16.0	beta2	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All

Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All

References

Reference	Source	Link
CVE-2019-11250: TOB-K8S-001: Bearer tokens are revealed in logs · Issue #81114 · kubernetes/kubernetes · GitHub	CONFIRM	github.c
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	access.
September 2019 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	security
Red Hat Customer Portal - Access to 24x7 support and knowledge	REDHAT	access.
oss-security - Kubernetes: Multiple secret leaks when verbose logging is enabled	MLIST	www.op
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[770012](#) Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2019:4087)

© [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](#)