



CVE-2019-3818

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

Summary

CVE	CVE-2019-3818
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-02-05 17:29:00 UTC
Updated	2021-05-21 14:42:00 UTC
Description	The kube-rbac-proxy container before version 0.4.1 as used in Red Hat OpenShift Container Platform does not honor TLS c

Risk And Classification

Problem Types: CWE-327

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kube-rbac-proxy Project	Kube-rbac-proxy	All	All	All	All
Application	Kubernetes	Kube-rbac-proxy	All	All	All	All
Application	Kubernetes	Kube-rbac-proxy	All	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All

References

Reference	Source
Red Hat Customer Portal	CON
Kube-rbac-proxy CVE-2019-3818 Information Disclosure Vulnerability	BID
1668961 – (CVE-2019-3818) CVE-2019-3818 kube-rbac-proxy: Improper application of config allows for insecure ciphers and TLS 1.0	CON
Red Hat Customer Portal	RED
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)