



CVE-2019-11253

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

Summary

CVE	CVE-2019-11253
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-10-17 16:15:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	Improper input validation in the Kubernetes API server in versions v1.0-1.12 and versions prior to v1.13.12, v1.14.8, v1.15.5

Risk And Classification

Problem Types: CWE-776

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
Application	Redhat	Openshift Container Platform	3.10	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.9	All	All	All
Application	Redhat	Openshift Container Platform	3.10	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	3.9	All	All	All

References

Reference

CVE-2019-11253: Kubernetes API Server JSON/YAML parsing vulnerable to resource exhaustion attack · Issue #83253 · kubernetes/kubernetes
Google Groups
Red Hat Customer Portal
Red Hat Customer Portal
Google Groups

Red Hat Customer Portal

CVE-2019-11253 Kubernetes Vulnerability in NetApp Products | NetApp Product Security

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Discovery Credit

LEGACY: Rory McCune

Legacy QID Mappings

500857 Alpine Linux Security Update for containerd
504639 Alpine Linux Security Update for containerd
770007 Red Hat OpenShift Container Platform 4.1.20 Security Update (RHSA-2019:3132)

© [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](#)