



CVE-2019-1002100

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

Summary

CVE	CVE-2019-1002100
State	PUBLIC
Assigner	cve-assign@distributedweaknessfiling.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-01 14:29:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	In all Kubernetes versions prior to v1.11.8, v1.12.6, and v1.13.4, users that are authorized to make patch requests to the Ku

Risk And Classification

Problem Types: CWE-770

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

References

Reference	Source	Li
Google Groups	CONFIRM	gr
April 2019 Kubernetes Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM	se
Google Groups		gr
Red Hat Customer Portal	REDHAT	ac
CVE-2019-1002100: json-patch requests can exhaust apiserver resources · Issue #74534 · kubernetes/kubernetes · GitHub	CONFIRM	git
Red Hat Customer Portal	REDHAT	ac
Kubernetes CVE-2019-1002100 Remote Denial of Service Vulnerability	BID	wv
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

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](#)