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	ww
CVE Program record	CVE.ORG	ww
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**