



CVE-2020-8554

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

Summary

CVE	CVE-2020-8554
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-21 17:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	Kubernetes API server in all versions allow an attacker who is able to create a ClusterIP service and set the spec.externalIP

Risk And Classification

Problem Types: NVD-CWE-noinfo

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	Oracle	Communications Cloud Native Core Network Slice Selection Function	1.2.1	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.15.0	All	All	All
Application	Oracle	Communications Cloud Native Core Service Communication Proxy	1.14.0	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mailing List, TI
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com	
Oracle Critical Patch Update Advisory - July 2021	N/A	www.oracle.com	
[Security Advisory] CVE-2020-8554: Man in the middle using LoadBalancer or ExternalIPs	MLIST	groups.google.com	Mailing List, TI
Pony Mail!		lists.apache.org	
Oracle Critical Patch Update Advisory - January 2022	MISC	www.oracle.com	
Pony Mail!		lists.apache.org	

RESERVED · Issue #97076 · kubernetes/kubernetes · GitHub	CONFIRM	github.com	Exploit, Third I
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mailing List, TI
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

Vendor Comments And Credit

Discovery Credit

LEGACY: Etienne Champetier (@champtar) of Anevia

Legacy QID Mappings

- [900263](#) CBL-Mariner Linux Security Update for kubernetes-1.18.17 1.18.17
- [900264](#) CBL-Mariner Linux Security Update for kubernetes 1.18.17
- [900265](#) CBL-Mariner Linux Security Update for kubernetes-1.18.14 1.18.14
- [900266](#) CBL-Mariner Linux Security Update for kubernetes-1.19.7 1.19.7
- [900267](#) CBL-Mariner Linux Security Update for kubernetes-1.19.9 1.19.9
- [900268](#) CBL-Mariner Linux Security Update for kubernetes-1.20.2 1.20.2
- [900269](#) CBL-Mariner Linux Security Update for kubernetes-1.20.5 1.20.5
- [900270](#) CBL-Mariner Linux Security Update for python-kubernetes 11.0.0
- [903524](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (6284)
- [905971](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (6284-1)
- [907546](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (31731-1)

© [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](#)