CVE-2020-8558

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-8558
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-27 20:15:00 UTC
Updated	2022-09-20 17:17:00 UTC
Description	The Kubelet and kube-proxy components in versions 1.1.0-1.16.10, 1.17.0-1.17.6, and 1.18.0-1.18.3 were found to contain

Risk And Classification

Problem Types: NVD-CWE-Other

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

References

Reference	S
[Security Advisory] CVE-2020-8558: Kubernetes: Node setting allows for neighboring hosts to bypass localhost boundary	M
CVE-2020-8558: Node setting allows for neighboring hosts to bypass localhost boundary · Issue #92315 · kubernetes/kubernetes · GitHub	C
CVE-2020-8558 Kubernetes Vulnerability in NetApp Products | NetApp Product Security	C
CVE Program record	C
NVD vulnerability detail	N

Vendor Comments And Credit

Discovery Credit

LEGACY: János Kövér, Ericsson

LEGACY: Additional impacts reported by Rory McCune, NCC Group and Yuval Avrahami and Ariel Zelivansky, Palo Alto Networks

Legacy QID Mappings

- 377856 Kubernetes kubelet Neighboring Hosts Bypass Vulnerability
- 6140289 AWS Bottlerocket Security Update for Kubernetes (GHSA-wqv3-8cm6-h6wg)
- 770028 Red Hat OpenShift Container Platform 4.5 Security Update (RHSA-2020:2413)
- 770034 Red Hat OpenShift Container Platform 4.4.13 Security Update (RHSA-2020:2927)
- 770035 Red Hat OpenShift Container Platform 4.3.31 Security Update (RHSA-2020:3183)
- 900220 CBL-Mariner Linux Security Update for kubernetes 1.16.10

© 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 registred 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