CVE-2021-25741

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-25741
State	PUBLIC
Assigner	security@kubernetes.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-20 17:15:00 UTC
Updated	2021-11-30 22:42:00 UTC
Description	A security issue was discovered in Kubernetes where a user may be able to create a container with subpath volume mounts

Risk And Classification

Problem Types: CWE-552

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	Kubernetes	Kubernetes	All	All	All	All

References

Reference	Source	Li
CVE-2021-25741 Kubernetes Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	se
CVE-2021-25741: Symlink Exchange Can Allow Host Filesystem Access · Issue #104980 · kubernetes/kubernetes · GitHub	CONFIRM	git
[Security Advisory] CVE-2021-25741: Symlink Exchange Can Allow Host Filesystem Access	MLIST	gro
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

LEGACY: Fabricio Voznika & Mark Wolters

Legacy QID Mappings

159556 Oracle Enterprise Linux Security Update for olcne (ELSA-2021-9526)

159558 Oracle Enterprise Linux Security Update for olcne istio istio kubernetes (ELSA-2021-9546)

180885 Debian Security Update for kubernetes (CVE-2021-25741)

239659 Red Hat Update for OpenShift Container Platform 3.11.524 (RHSA-2021:3646)

239660 Red Hat Update for OpenShift Container Platform 4.6.46 (RHSA-2021:3642)

239661 Red Hat Update for OpenShift Container Platform 4.7.32 packages and (RHSA-2021:3635)

239662 Red Hat Update for OpenShift Container Platform 4.8.13 (RHSA-2021:3631)

375921 Kubernetes Improper Authorization Vulnerability

6140357 AWS Bottlerocket Security Update for kubernetes (GHSA-f5f7-6478-qm6p)

770079 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021:3642)

770080 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021:3631)

770081 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021:3635)

770089 Red Hat OpenShift Container Platform 4.8 Security Update (RHSA-2021-3631)

770097 Red Hat OpenShift Container Platform 4.7 Security Update (RHSA-2021-3635)

770114 Red Hat OpenShift Container Platform 4.6 Security Update (RHSA-2021-3642)

900356 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (6285)

900844 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.19.13 (5912)

900846 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.21.1 (5915)

900847 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.19.11 (5911)

900848 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.21.2 (5916)

900849 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.20.7 (5913)

900851 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes-1.20.9 (5914)

906026 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (6285-1)

980239 Go (go) Security Update for k8s.io/kubernetes (GHSA-f5f7-6478-qm6p)

© 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