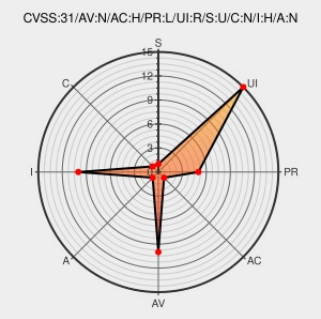
CVE-2019-11251

Published on: 02/03/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:36 PM UTC

CVE-2019-11251

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Kubernetes from Kubernetes contain the following vulnerability:

The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.

CVE-2019-11251 has been assigned by security@kubernetes.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.7 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	HIGH	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Google Groups	Mailing List Third Party Advisory	MLIST Security release of kubectl versions v1.16.0 / 1.15.4 / 1.14.7 and 1.13.11 - CVE-2019-11251

	groups.google.com text/html	
CVE-2019-11251: kubectl cp symlink vulnerability · Issue #87773 · kubernetes/kubernetes · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/kubernetes/kubernetes/issues/87773

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

770008 Red Hat OpenShift Container Platform 4.1 Security Update (RHSA-2019:3266)

982577 Go (go) Security Update for github.com/kubernetes/kubernetes/pkg/kubectl/cmd/cp (GHSA-6qfg-8799-r575)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.1-1.12	All	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.1-1.12	All	All	All

cpe:2.3:a:kubernetes:kubernetes:*:*:*:*:*:*:*:*:

cpe:2.3:a:kubernetes:kubernetes:1.1-1.12:*:*:*:*:*:*:*:

cpe:2.3:a:kubernetes:kubernetes:*:*:*:*:*:*:*:*:

cpe:2.3:a:kubernetes:kubernetes:1.1-1.12:*:*:*:*:*:*:*:

Discovery Credit

Erik Sjölund

Social Mentions

Source	Title	Posted (UTC)
/r/TutorialBoy	A Detailed Talk about K8S Cluster Security from the Perspective of Attackers (Part 1)	2022-09-15 17:54:15

← Previous ID

Next ID→

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