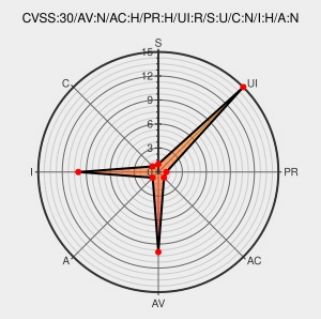
CVE-2018-1002100

Published on: 06/01/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:37 PM UTC

CVE-2018-1002100

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



Certain versions of Kubernetes from Kubernetes contain the following vulnerability:

In Kubernetes versions 1.5.x, 1.6.x, 1.7.x, 1.8.x, and prior to version 1.9.6, the kubectl cp command insecurely handles tar data returned from the container, and can be caused to overwrite arbitrary local files.

CVE-2018-1002100 has been assigned by jordan@liggitt.net to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Kubernetes** - **Kubernetes** version = **v1.5.x**

Affected Vendor/Software: **Kubernetes** - **Kubernetes** version = **v1.6.x**

Affected Vendor/Software: **Kubernetes** - **Kubernetes** version = **v1.7.x**

Affected Vendor/Software: **Kubernetes** - **Kubernetes** version = **v1.8.x**

Affected Vendor/Software: **Kubernetes** - **Kubernetes** version < **v1.9.6**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 3.6 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE | PARTIAL | PARTIAL

CVE References

Description	Tags	Link
Kubectl copy doesn't check for paths outside of it's destination directory. · Issue #61297 · kubernetes/kubernetes · GitHub	Third Party Advisory, github.com, text/html	CONFIRM github.com/kubernetes/kubernetes/issues/61297
OpenShift S2I privilege escalation vulnerability	Third Party Advisory, hansmi.ch, text/html	MISC hansmi.ch/articles/2018-04-openshift-s2i-security
Bug 1564305 – CVE-2018-1002100 kubernetes: Kubectl copy doesn't check for paths outside of it's destination directory	Issue Tracking, Third Party Advisory, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1564305

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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
Application	Kubernetes	Kubernetes	All	All	All	All

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

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

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

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

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

Discovery Credit

Array

Social Mentions

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

/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→