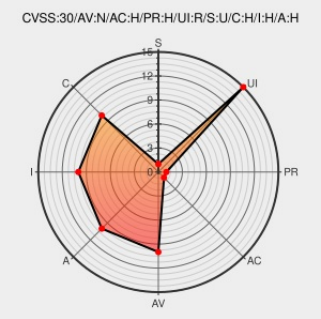
CVE-2019-11246

Published on: 08/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:35 PM UTC

CVE-2019-11246 - advisory for

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



Certain versions of Kubernetes from Kubernetes contain the following vulnerability:

The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes runs tar inside the container to create a tar archive, copies it over the network, and kubectl unpacks it on the user's machine. If the tar binary in the container is malicious, it could run any code and output unexpected, malicious results. An attacker could use this to write files to any path on the user's machine when kubectl cp is called, limited only by the system permissions of the local user. Kubernetes affected versions include versions prior to 1.12.9, versions prior to 1.13.6, versions prior to 1.14.2, and versions 1.1, 1.2, 1.4, 1.4, 1.5, 1.6, 1.7, 1.8, 1.9, 1.10, 1.11.

CVE-2019-11246 has been assigned by security@kubernetes.io to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	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
CVE-2019-11246: Clean links handling in cp's tar code by soltysh · Pull Request #76788 · kubernetes/kubernetes · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/kubernetes/kubernetes/pull/76788
September 2019 Kubernetes Vulnerabilities in NetApp Products | NetApp Product Security	Third Party Advisory security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20190919-0003/
Google Groups	Third Party Advisory groups.google.com text/html	MLIST [ANNOUNCE] Incomplete fixes for CVE-2019-1002101, kubectl cp potential directory traversal - CVE-2019-11246

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	1.12.11	beta0	All	All
Application	Kubernetes	Kubernetes	All	All	All	All
Application	Kubernetes	Kubernetes	1.12.11	beta0	All	All
Application	Kubernetes	Kubernetes	All	All	All	All

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

cpe:2.3:a:kubernetes:kubernetes:1.12.11:beta0:*:*:*:*:*:*:

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

cpe:2.3:a:kubernetes:kubernetes:1.12.11:beta0:*:*:*:*:*:*:

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

Discovery Credit

Charles Holmes, Atredis Partners

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→