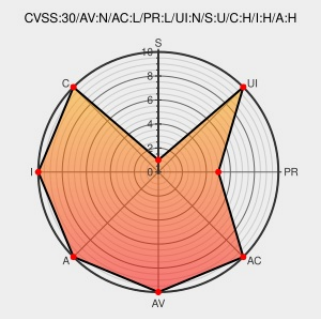
CVE-2017-1002101

Published on: 03/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:39 PM UTC

CVE-2017-1002101

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



Certain versions of Kubernetes from Kubernetes contain the following vulnerability:

In Kubernetes versions 1.3.x, 1.4.x, 1.5.x, 1.6.x and prior to versions 1.7.14, 1.8.9 and 1.9.4 containers using subpath volume mounts with any volume type (including non-privileged pods, subject to file permissions) can access files/directories outside of the volume, including the host's filesystem.

CVE-2017-1002101 has been assigned by security@kubernetes.io to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.6 - CRITICAL

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2020:0554-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0554
CVE-2017-1002101 - subpath volume mount handling allows	Issue Tracking	CONFIRM

CVE-2017-1002101 - subpath volume mount handling allows arbitrary file access in host filesystem · Issue #60813 · kubernetes/kubernetes · GitHub	Issue Tracking Mitigation Vendor Advisory github.com text/html	CONFIRM github.com/kubernetes/kubernetes/issues/60813
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2018:0475
GitHub - bgeesaman/subpath-exploit: Writeup of CVE-2017-1002101 with sample "exploit"/escape	Exploit Third Party Advisory github.com text/html	MISC github.com/bgeesaman/subpath-exploit/

Related QID Numbers

377879 Kubernetes Arbitrary File Access Vulnerability

Exploit/POC from Github

Writeup of CVE-2017-1002101 with sample "exploit"/escape

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
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:*:*:*:*:*:*:*:*:

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

Discovery Credit

Array

Social Mentions

Source	Title	Posted (UTC)
@yawaramin	I mean, - CVE-2017-1002101 - subpath volume mount handling allows arbitrary file access in host filesystem - CVE-20… twitter.com/i/web/status/1…	2021-10-03 16:21:17
/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→