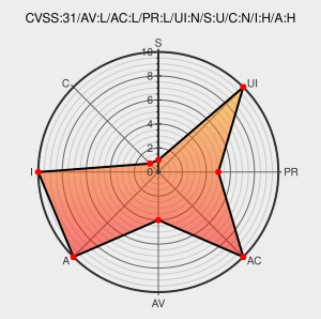
CVE-2020-28914

Published on: 11/17/2020 12:00:00 AM UTC

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

CVE-2020-28914

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



Certain versions of Kata-containers from Katacontainers contain the following vulnerability:

An improper file permissions vulnerability affects Kata Containers prior to 1.11.5. When using a Kubernetes hostPath volume and mounting either a file or directory into a container as readonly, the file/directory is mounted as readOnly inside the container, but is still writable inside the guest. For a container breakout situation, a malicious guest can potentially modify or delete files/directories expected to be read-only.

CVE-2020-28914 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

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

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
Backports: Read-only mount fixes for 1.11 by amshinde · Pull Request #3051 · kata-containers/runtime · GitHub	Third Party Advisory github.com	MISC github.com/kata-containers/runtime/pull/3051

	text/html	
Release # Release 1.12.0 · kata-containers/runtime · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/releases/tag/1.12.0
readonly volume should be bind mounted readonly on the host by bergwolf · Pull Request #3042 · kata-containers/runtime · GitHub	Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/pull/3042
Release # Release 1.11.5 · kata-containers/runtime · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/releases/tag/1.11.5
runtime: readonly volume should be bind mounted readonly on the host by bergwolf · Pull Request #1062 · kata-containers/kata-containers · GitHub	Third Party Advisory github.com text/html	MISC github.com/kata-containers/kata-containers/pull/1062

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Katacontainers	Kata-containers	All	All	All	All
Application	Katacontainers	Kata-containers	All	All	All	All

cpe:2.3:a:katacontainers:kata-containers:*:*:*:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata-containers:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@securibee	@Bugcrowd Big bugs - bitbucket pipelines kata containers build container escape: bugcrowd.com/blog/big-bugs-…	2021-05-12 14:25:28

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report