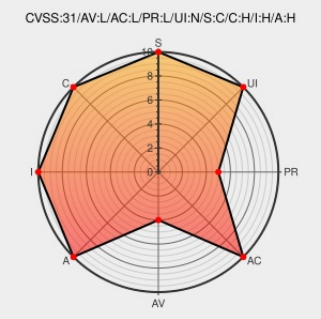
CVE-2020-2025

Published on: 05/19/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:08 PM UTC

CVE-2020-2025

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



Certain versions of Runtime from Katacontainers contain the following vulnerability:

Kata Containers before 1.11.0 on Cloud Hypervisor persists guest filesystem changes to the underlying image file on the host. A malicious guest can overwrite the image file to gain control of all subsequent guest VMs. Since Kata Containers uses the same VM image file with all VMMs, this issue may also affect QEMU and Firecracker based guests.

CVE-2020-2025 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Kata Containers** - **Kata Containers** version **< 1.11.0**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link

clh: update CLH to stable/v0.5.x by likebreath · Pull Request #2487 · kata-containers/runtime · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/pull/2487

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Katacontainers	Runtime	All	All	All	All
Application	Katacontainers	Runtime	All	All	All	All

cpe:2.3:a:katacontainers:runtime:*:*:*:*:*:*:*:*:

cpe:2.3:a:katacontainers:runtime:*:*:*:*:*:*:*:*:

Discovery Credit

Yuval Avrahami, Palo Alto Networks

← Previous ID

Next ID→