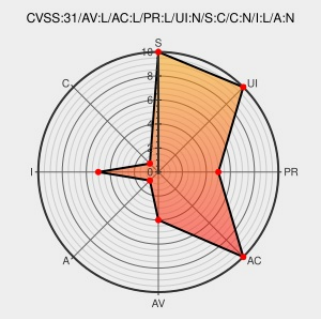
CVE-2020-2023

Published on: 06/10/2020 12:00:00 AM UTC

Last Modified on: 10/19/2021 12:45:00 PM UTC

CVE-2020-2023

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



Certain versions of Runtime from Katacontainers contain the following vulnerability:

Kata Containers doesn't restrict containers from accessing the guest's root filesystem device. Malicious containers can exploit this to gain code execution on the guest and masquerade as the kata-agent. This issue affects Kata Containers 1.11 versions earlier than 1.11.1; Kata Containers 1.10 versions earlier than 1.10.5; and Kata Containers 1.9 and earlier versions.

CVE-2020-2023 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Kata Containers** - **Kata Containers** version **< 1.11.1**

Affected Vendor/Software: **Kata Containers** - **Kata Containers** version **< 1.10.5**

Affected Vendor/Software: **Kata Containers** - **Kata Containers** version **<= 1.9**

CVSS3 Score: 6.3 - MEDIUM

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

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
clh: update CLH to stable/v0.5.x · Issue #2488 · kata-containers/runtime · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/issues/2488
Explicitly deny any access to the nvdimm root partition · Issue #791 · kata-containers/agent · GitHub	Third Party Advisory github.com text/html	MISC github.com/kata-containers/agent/issues/791
Release # Release 1.10.5 · kata-containers/runtime · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/releases/tag/1.10.5
device: Do not allow container access to the nvdimm rootfs by amshinde · Pull Request #792 · kata-containers/agent · GitHub	Patch github.com text/html	MISC github.com/kata-containers/agent/pull/792
qemu: pass rootfs image in readonly mode by bergwolf · Pull Request #2477 · kata-containers/runtime · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/pull/2477
Release # Release 1.11.1 · kata-containers/runtime · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/releases/tag/1.11.1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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
Application	Katacontainers	Runtime	All	All	All	All

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

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

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

Discovery Credit

Discovery Credit

Yuval Avrahami, Palo Alto Networks

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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