



CVE-2020-2024

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

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

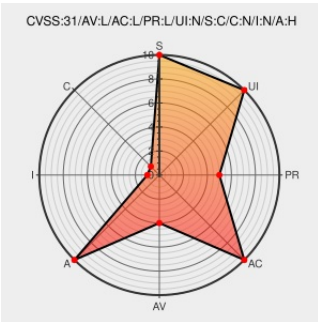
CVE-2020-2024

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Runtime](#) from [Katacontainers](#) contain the following vulnerability:

An improper link resolution vulnerability affects Kata Containers versions prior to 1.11.0. Upon container teardown, a malicious guest can trick the kata-runtime into unmounting any mount point on the host and all mount points underneath it, potentiality resulting in a host DoS.

CVE-2020-2024 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as **MEDIUM** severity.

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

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

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

CVE References

Description	Tags	Link
harden container hostpath cleanup · Issue #2474 · kata-containers/runtime · GitHub	Third Party Advisory github.com text/html	MISC github.com/kata-containers/runtime/issues/2474

vc: do not follow symlink when umounting container host path by bergwolf · Pull Request #2475 · kata-containers/runtime · GitHub

Patch

CONFIRM N/A

Third Party Advisory

github.com

text/html

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

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

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

Discovery Credit

Yuval Avrahami, Palo Alto Networks

[← 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 registered 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](#)