



CVE-2020-27151

Published on: 12/07/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:28 PM UTC

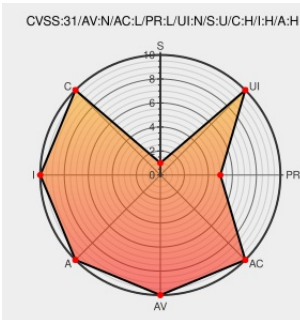
CVE-2020-27151

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

An issue was discovered in Kata Containers through 1.11.3 and 2.x through 2.0-rc1. The runtime will execute binaries given using annotations without any kind of validation. Someone who is granted access rights to a cluster will be able to have kata-runtime execute arbitrary binaries as root on the worker nodes.

CVE-2020-27151 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **9 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Release Kata Containers 2.0.0 · kata-containers/kata-containers · GitHub	Third Party Advisory github.com text/html	MISC github.com/kata-containers/kata-containers/releases/tag/2.0.0

Release # Release 1.12.0 · kata-containers/runtime · GitHub

Third Party Advisory
github.com
text/html

MISC github.com/kata-containers/runtime/releases/tag/1.12.0

Bug #1878234 "Some kata-runtime annotations can execute arbitrar..." : Bugs : Kata Containers

Exploit
Issue Tracking
Third Party Advisory
bugs.launchpad.net
text/html

MISC bugs.launchpad.net/katacontainers.io/+bug/1878234

Release # Release 1.11.5 · kata-containers/runtime · GitHub

Third Party Advisory
github.com
text/html

MISC github.com/kata-containers/runtime/releases/tag/1.11.5

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	Kata Containers	2.0.0	alpha1	All	All
Application	Katacontainers	Kata Containers	2.0.0	alpha2	All	All
Application	Katacontainers	Kata Containers	2.0.0	alpha3	All	All
Application	Katacontainers	Kata Containers	2.0.0	rc0	All	All
Application	Katacontainers	Kata Containers	2.0.0	rc1	All	All
Application	Katacontainers	Kata Containers	2.0.0	alpha1	All	All
Application	Katacontainers	Kata Containers	2.0.0	alpha2	All	All
Application	Katacontainers	Kata Containers	2.0.0	alpha3	All	All
Application	Katacontainers	Kata Containers	2.0.0	rc0	All	All
Application	Katacontainers	Kata Containers	2.0.0	rc1	All	All
Application	Katacontainers	Kata Containers	All	All	All	All

cpe:2.3:a:katacontainers:kata_containers:2.0.0:alpha1:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:alpha2:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:alpha3:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:rc0:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:rc1:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:alpha1:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:alpha2:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:alpha3:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:rc0:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:2.0.0:rc1:*:*:*:*:*:

cpe:2.3:a:katacontainers:kata_containers:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← 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](#)