



CVE-2020-2026

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

Last Modified on: 11/16/2022 03:40:00 AM UTC

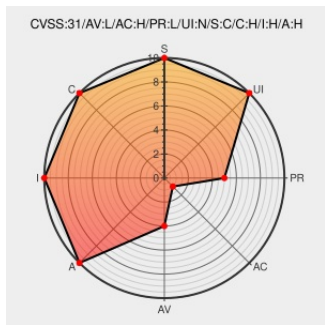
CVE-2020-2026

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

A malicious guest compromised before a container creation (e.g. a malicious guest image or a guest running multiple containers) can trick the kata runtime into mounting the untrusted container filesystem on any host path, potentially allowing for code execution on the host. This issue affects: Kata Containers 1.11 versions earlier than 1.11.1; Kata Containers 1.10 versions earlier than 1.10.5; Kata Containers 1.9 and earlier versions.

CVE-2020-2026 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as **HIGH** severity.

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

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

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











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
[SECURITY] Fedora 31 Update: kata-shim-1.11.1-1.fc31.1 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-1af9cd8c87
[SECURITY] Fedora 31 Update: kata-proxy-1.11.1-1.fc31.1 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-2f5879aeb6
vc: make host shared path readonly by bergwolf · Pull Request #2713 · kata-containers/runtime · GitHub	Third Party Advisory github.com text/html	 MISC github.com/kata-containers/runtime/pull/2713
host shared directory should be readonly · Issue #2712 · kata-containers/runtime · GitHub	Third Party Advisory github.com text/html	 MISC github.com/kata-containers/runtime/issues/2712
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
[SECURITY] Fedora 31 Update: kata-agent-1.11.1-1.fc31.1 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-c33083813d
[SECURITY] Fedora 31 Update: kata-runtime-1.11.1-3.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-7a0b6071a4
[SECURITY] Fedora 31 Update: kata-ksm-throttler-1.11.1-1.fc31.1 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-15a1bde727
[SECURITY] Fedora 31 Update: kata-osbuilder-1.11.1-1.fc31.1 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-61fcf3fc7
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
Operating System	Fedoraproject	Fedora	31	All	All	All
Application	Katacontainers	Runtime	All	All	All	All
Application	Katacontainers	Runtime	All	All	All	All
Application	Katacontainers	Runtime	All	All	All	All

cpe:2.3:o:fedoraproject:fedora:31:*:*:*:*:*:

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

