

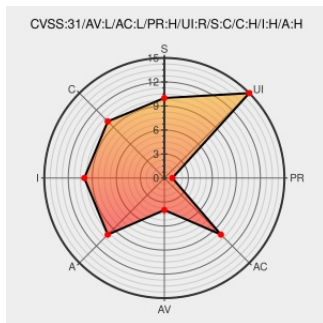


CVE-2019-10144

Published on: 06/03/2019 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:06:59 PM UTC

CVE-2019-10144

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Rkt](#) from [Redhat](#) contain the following vulnerability: rkt through version 1.30.0 does not isolate processes in containers that are run with ``rkt enter``. Processes run with ``rkt enter`` are given all capabilities during stage 2 (the actual environment in which the applications run). Compromised containers could exploit this flaw to access host resources.

CVE-2019-10144 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **[UNKNOWN]** - rkt version = 1.30.0

CVSS3 Score: **7.7 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.9 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Comprehensive Cloud Security Prisma - Palo Alto Networks	Exploit Third Party Advisory www.twistlock.com	MISC www.twistlock.com/labs-blog/breaking-out-of-coresos-rkt-3-new-cves/

www.mitre.org

text/html

1711905 – (CVE-2019-10144) CVE-2019-10144 rkt: processes run with `rkt enter` are given all capabilities during stage 2

Issue Tracking

Third Party Advisory

bugzilla.redhat.com

text/html

CONFIRM

bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10144

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	Redhat	Rkt	All	All	All	All

cpe:2.3:a:redhat:rkt:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →