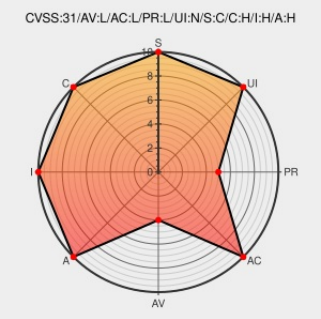
CVE-2020-14298

Published on: 07/13/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:39:00 PM UTC

CVE-2020-14298

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



Certain versions of Docker from Docker contain the following vulnerability:

The version of docker as released for Red Hat Enterprise Linux 7 Extras via RHBA-2020:0053 advisory included an incorrect version of runc missing the fix for CVE-2019-5736, which was previously fixed via RHSA-2019:0304. This issue could allow a malicious or compromised container to compromise the container host and other containers running on the same host. This issue only affects docker version 1.13.1-108.git4ef4b30.el7, shipped in Red Hat Enterprise Linux 7 Extras. Both earlier and later versions are not affected.

CVE-2020-14298 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

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
1848239 - (CVE-2020-14298) CVE-2020-14298		MISC bugzilla.redhat.com/show_bug.cgi?

1848239 – (CVE-2020-14298) CVE-2020-14298 docker: Security regression of CVE-2019-5736 due to inclusion of vulnerable runc	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1848239
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	CONFIRM access.redhat.com/errata/RHBA-2020:0427
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2020:2653
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	CONFIRM access.redhat.com/security/cve/CVE-2020-14298
1664908 – (CVE-2019-5736) CVE-2019-5736 runc: Execution of malicious containers allows for container escape and access to host filesystem	Issue Tracking Patch Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-5736
Runc regression - docker-1.13.1-108 - CVE-2016-8867, CVE-2020-14298, and CVE-2020-14300 - Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	MISC access.redhat.com/security/vulnerabilities/runc-regression-docker-1.13.1-108
runc - Malicious container escape - CVE-2019-5736 - Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	CONFIRM access.redhat.com/security/vulnerabilities/runcescape

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Docker	Docker	1.13.1	All	All	All
Application	Docker	Docker	1.13.1	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Application	Redhat	Openshift Container Platform	All	All	All	All

cpe:2.3:a:docker:docker:1.13.1:*:*:*:*:*:*:*:

cpe:2.3:a:docker:docker:1.13.1:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/devopsish	runc regression - docker-1.13.1-108 - CVE-2016-8867, CVE-2020-14298, and CVE-2020-14300	2020-06-23 22:24:08

← Previous ID

Next ID→