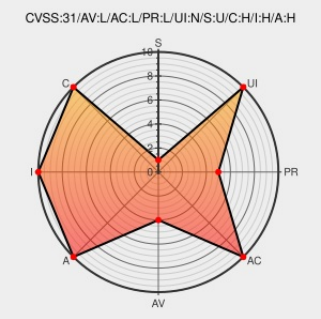
CVE-2019-19350

Published on: 03/24/2021 12:00:00 AM UTC

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

CVE-2019-19350

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



Certain versions of Openshift from Redhat contain the following vulnerability:

An insecure modification vulnerability in the /etc/passwd file was found in the openshift/ansible-service-broker as shipped in Red Hat Openshift 4 and 3.11. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.

CVE-2019-19350 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	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
1791534 – OpenShift: containers modify /etc/passwd group writable	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1791534
1793283 – (CVE-2019-19350) CVE-2019-19350 openshift/ansible-service-	bugzilla.redhat.com	MISC

broker: /etc/passwd is given incorrect privileges	text/html	bugzilla.redhat.com/show_bug.cgi?id=1793283

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Openshift	3.11	All	All	All
Application	Redhat	Openshift	4.0	All	All	All

cpe:2.3:a:redhat:openshift:3.11:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift:4.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→