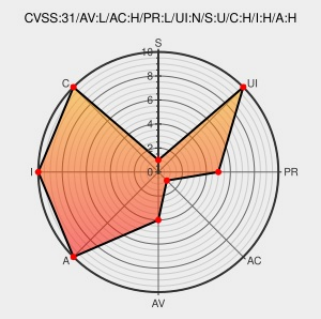
CVE-2020-1706

Published on: 03/09/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:40:00 PM UTC

CVE-2020-1706

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



Certain versions of Openshift Container Platform from Redhat contain the following vulnerability:

It has been found that in openshift-enterprise version 3.11 and openshift-enterprise versions 4.1 up to, including 4.3, multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/apb-tools-container.

CVE-2020-1706 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Red Hat** - **openshift/apb-tools-container** version **= openshift-enterprise version 3.11**

Affected Vendor/Software: **Red Hat** - **openshift/apb-tools-container** version **= from openshift-enterprise version 4.1 to, including 4.3**

CVSS3 Score: 7 - HIGH

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

CVSS2 Score: 4.4 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2020:2305
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2020:2442
1793302 – (CVE-2020-1706) CVE-2020-1706 openshift/apb-tools: /etc/passwd is given incorrect privileges	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1706
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2020-1706
1793302 – (CVE-2020-1706) CVE-2020-1706 openshift/apb-tools: /etc/passwd is given incorrect privileges	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1793302
OpenShift Containers - Modification of /etc/passwd - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/articles/4859371

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 Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	4.2	All	All	All
Application	Redhat	Openshift Container Platform	4.3	All	All	All
Application	Redhat	Openshift Container Platform	3.11	All	All	All
Application	Redhat	Openshift Container Platform	4.1	All	All	All
Application	Redhat	Openshift Container Platform	4.2	All	All	All
Application	Redhat	Openshift Container Platform	4.3	All	All	All

cpe:2.3:a:redhat:openshift_container_platform:3.11:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:3.11:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.1:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.2:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→