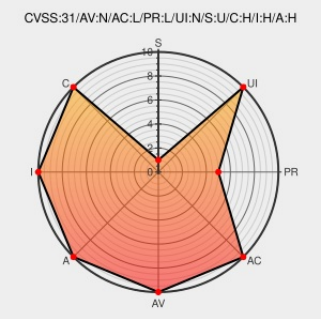
CVE-2021-20182

Published on: 02/23/2021 12:00:00 AM UTC

Last Modified on: 05/21/2021 03:28:00 PM UTC

CVE-2021-20182

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



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

A privilege escalation flaw was found in openshift4/ose-docker-builder. The build container runs with high privileges using a chrooted environment instead of runc. If an attacker can gain access to this build container, they can potentially utilize the raw devices of the underlying node, such as the network and storage devices, to at least escalate their privileges to that of the cluster admin. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2021-20182 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
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
1915110 - (CVE-2021-20182) CVE-2021-20182 openshift: builder allows read		MISC

1915110 – (CVE-2021-20182) CVE-2021-20182 openshift: builder allows read and write of block devices

Issue Tracking
Mitigation
Patch
Vendor Advisory
bugzilla.redhat.com
text/html

MISC
bugzilla.redhat.com/show_bug.cgi?id=1915110

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	All	All	All	All
Application	Redhat	Openshift Container Platform	4.4	All	All	All
Application	Redhat	Openshift Container Platform	4.5	All	All	All
Application	Redhat	Openshift Container Platform	4.6	All	All	All
Application	Redhat	Openshift Container Platform	4.4	All	All	All
Application	Redhat	Openshift Container Platform	4.5	All	All	All
Application	Redhat	Openshift Container Platform	4.6	All	All	All

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

cpe:2.3:a:redhat:openshift_container_platform:4.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.6:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_container_platform:4.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report