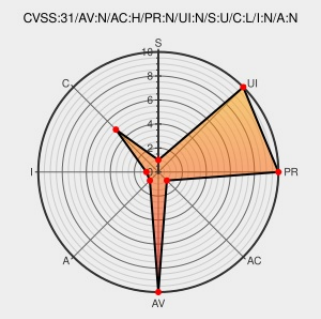
CVE-2021-20238

Published on: Not Yet Published

Last Modified on: 06/26/2023 06:00:00 PM UTC

CVE-2021-20238

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



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

It was found in OpenShift Container Platform 4 that ignition config, served by the Machine Config Server, can be accessed externally from clusters without authentication. The MCS endpoint (port 22623) provides ignition configuration used for bootstrapping Nodes and can include some sensitive data, e.g. registry pull secrets. There are two scenarios where this data can be accessed. The first is on Baremetal, OpenStack, Ovirt, Vsphere and KubeVirt deployments which do not have a separate internal API endpoint and allow access from outside the cluster to port 22623 from the standard OpenShift API Virtual IP address. The second is on cloud deployments when using unsupported network plugins, which do not create iptables rules that prevent to port 22623. In this scenario, the ignition config is exposed to all pods within the cluster and cannot be accessed externally.

CVE-2021-20238 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.7 - LOW

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
1926568 – (CVE-2021-20238) CVE-2021-20238 openshift/machine-config-operator: unauthenticated access to Machine Config Server ignition config	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1926568

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	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Machine-config-operator	All	All	All	All

cpe:2.3:a:redhat:openshift_container_platform:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openshift_machine-config-operator:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-20238 : It was found in OpenShift Container Platform 4 that ignition config, served by the Machine Config… twitter.com/i/web/status/1…	2022-04-01 23:18:39
/r/netcve	CVE-2021-20238	2022-04-01 23:38:40

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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