

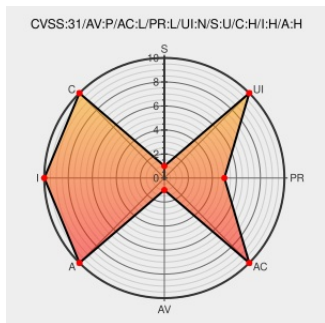


CVE-2020-10706

Published on: 05/12/2020 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:38:00 PM UTC

CVE-2020-10706

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [OpenShift Container Platform](#) from [Redhat](#) contain the following vulnerability:

A flaw was found in OpenShift Container Platform where OAuth tokens are not encrypted when the encryption of data at rest is enabled. This flaw allows an attacker with access to a backup to obtain OAuth tokens and then use them to log into the cluster as any user who logged into the cluster via the WebUI or via the command line in the last 24 hours.

Once the backup is older than 24 hours the OAuth tokens are no longer valid.

CVE-2020-10706 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **[UNKNOWN]** - [openshift/openshift-apiser](#) version = n/a

CVSS3 Score: **6.6 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	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
-------------	------	------

1819011 – (CVE-2020-10706) CVE-2020-10706 openshift/openshift-apiserver: oauth tokens not encrypted when enabling encryption of data at rest	bugzilla.redhat.com text/html	 MISC bugzilla.redhat.com/show_bug.cgi?id=1819011
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/security/cve/CVE-2020-10706
1819011 – (CVE-2020-10706) CVE-2020-10706 openshift/openshift-apiserver: oauth tokens not encrypted when enabling encryption of data at rest	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10706
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	 MISC access.redhat.com/errata/RHBA-2020:4196
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	-	All	All	All
Application	Redhat	Openshift Container Platform	-	All	All	All
cpe:2.3:a:redhat:openshift_container_platform:-:~::~~::~~::~~::~~::~~::~~::						
cpe:2.3:a:redhat:openshift_container_platform:-:~::~~::~~::~~::~~::~~::~~::						

No vendor comments have been submitted for this CVE

[← 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 registered 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](#)