



CVE-2018-1085

Published on: 06/15/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:31 PM UTC

CVE-2018-1085

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

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

openshift-ansible before versions 3.9.23, 3.7.46 deploys a misconfigured etcd file that causes the SSL client certificate authentication to be disabled. Quotations around the values of ETCD_CLIENT_CERT_AUTH and ETCD_PEER_CLIENT_CERT_AUTH in etcd.conf result in etcd being

configured to allow remote users to connect without any authentication if they can access the etcd server bound to the network on the master nodes. An attacker could use this flaw to read and modify all the data about the OpenShift cluster in the etcd datastore, potentially adding another compute node, or bringing down the entire cluster.

CVE-2018-1085 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **[UNKNOWN]** - **openshift-ansible** version **openshift-ansible 3.9.23-1**

Affected Vendor/Software: **[UNKNOWN]** - **openshift-ansible** version **openshift-ansible 3.7.46-1**

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	 REDHAT RHSA-2018:2013
1557822 – (CVE-2018-1085) CVE-2018-1085 openshift-ansible: Incorrectly quoted values in etcd.conf causes disabling of SSL client certificate authentication	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	 CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-1085

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	All
Application	Redhat	Openshift Container Platform	All	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 →