

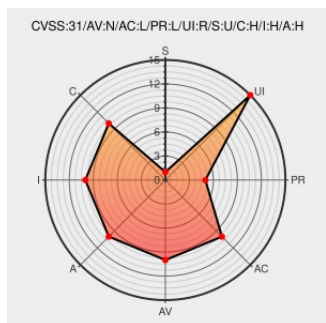


CVE-2019-3895

Published on: 06/03/2019 12:00:00 AM UTC

Last Modified on: 08/04/2021 05:14:00 PM UTC

CVE-2019-3895

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

Certain versions of [Octavia](#) from [Openstack](#) contain the following vulnerability:

An access-control flaw was found in the Octavia service when the cloud platform was deployed using Red Hat OpenStack Platform Director. An attacker could cause new amphorae to run based on any arbitrary image. This meant that a remote attacker could upload a new amphorae image and, if requested to spawn new amphorae, Octavia would then pick up the compromised image.

CVE-2019-3895 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Red Hat** - **openstack-tripleo-common** version **n/a**

CVSS3 Score: **8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

1694608 – (CVE-2019-3895) CVE-2019-3895 openstack-tripleo-common:
Allows running new amphorae based on arbitrary images

Issue Tracking

Mitigation

Third Party Advisory

bugzilla.redhat.com

text/html

CONFIRM

bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3895

Red Hat Customer Portal

Third Party Advisory

access.redhat.com

text/html

REDHAT RHSA-2019:1742

Red Hat Customer Portal

Third Party Advisory

access.redhat.com

text/html

REDHAT RHSA-2019:1683

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	Openstack	Octavia	All	All	All	All
Application	Openstack	Octavia	All	All	All	All
Application	Redhat	Openstack	12	All	All	All
Application	Redhat	Openstack	12.0	All	All	All
Application	Redhat	Openstack	12.0	All	All	All

cpe:2.3:a:openstack:octavia:*****:

cpe:2.3:a:openstack:octavia:*****:

cpe:2.3:a:redhat:openstack:12:*****:

cpe:2.3:a:redhat:openstack:12.0:*****:

cpe:2.3:a:redhat:openstack:12.0:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

[site](#). This site includes MITRE data granted under the following [license](#).

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