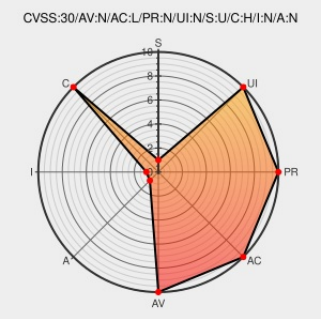
CVE-2018-16856

Published on: 03/26/2019 12:00:00 AM UTC

Last Modified on: 08/04/2021 05:15:00 PM UTC

CVE-2018-16856

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



Certain versions of Octavia from Openstack contain the following vulnerability:

In a default Red Hat Openstack Platform Director installation, openstack-octavia before versions openstack-octavia 2.0.2-5 and openstack-octavia-3.0.1-0.20181009115732 creates log files that are readable by all users. Sensitive information such as private keys can appear in these log files allowing for information exposure.

CVE-2018-16856 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **[UNKNOWN]** - **openstack-octavia** version **2.0.2-5**

Affected Vendor/Software: **[UNKNOWN]** - **openstack-octavia** version **openstack-octavia-3.0.1-0.20181009115732**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link

Description	Tags	Link
1649165 – (CVE-2018-16856) CVE-2018-16856 openstack-octavia: Private keys written to world-readable log files	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16856

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	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	14	All	All	All
Application	Redhat	Openstack	14.0	All	All	All
Application	Redhat	Openstack	12.0	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	14.0	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:13:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:13.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:14:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:14.0:*:*:*:*:*:*:*:

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

cpe:2.3:a:redhat:openstack:13.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack:14.0:*:*:*:*:*:*:*:

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 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