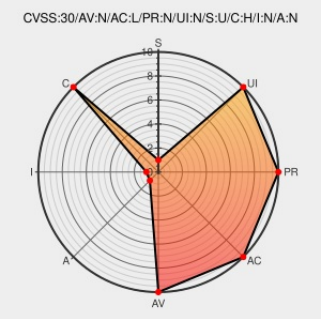
CVE-2018-16849

Published on: 11/02/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

CVE-2018-16849

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



Certain versions of Openstack-mistral from Redhat contain the following vulnerability:

A flaw was found in openstack-mistral. By manipulating the SSH private key filename, the std.ssh action can be used to disclose the presence of arbitrary files within the filesystem of the executor running the action. Since std.ssh private_key_filename can take an absolute path, it can be used to assess whether or not a file exists on the executor's filesystem.

CVE-2018-16849 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **[UNKNOWN]** - **openstack-mistral** version **n/a**

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

Bug #1783708 “std.ssh action can be used to explore executor's f...” : Bugs : Mistral	Third Party Advisory bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/mistral/+bug/1783708
1645334 – (CVE-2018-16849) CVE-2018-16849 openstack-mistral: std.ssh action may disclose presence of arbitrary files	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16849

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	Openstack-mistral	All	All	All	All
Application	Redhat	Openstack-mistral	All	All	All	All

cpe:2.3:a:redhat:openstack-mistral:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:openstack-mistral:*:*:*:*:*:*:*:*:

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