



CVE-2018-16848

Published on: 06/15/2020 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:08:09 AM UTC

CVE-2018-16848

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Openstack-mistral](#) from [Redhat](#) contain the following vulnerability:

A Denial of Service (DoS) condition is possible in OpenStack Mistral in versions up to and including 7.0.3. Submitting a specially crafted workflow definition YAML file containing nested anchors can lead to resource exhaustion culminating in a denial of service.

CVE-2018-16848 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
Bug #1785657 "Denial of service through YAML anchors expansion (...": Bugs : Mistral	Third Party Advisory bugs.launchpad.net text/html	MISC bugs.launchpad.net/mistral/+bug/1785657
1645332 – (CVE-2018-16848) CVE-2018-16848 openstack-mistral:	Issue Tracking	MISC

Potential Mistral Denial of Service handling recursive YAML anchor expansion

Vendor Advisory

bugzilla.redhat.com

text/html

bugzilla.redhat.com/show_bug.cgi?id=1645332

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
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 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](#)