

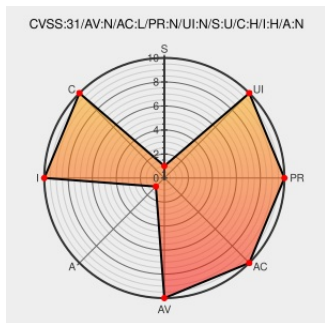


CVE-2019-17134

Published on: 10/08/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:38 PM UTC

CVE-2019-17134

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

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

Amphora Images in OpenStack Octavia $\geq 0.10.0$ $< 2.1.2$, $\geq 3.0.0$ $< 3.2.0$, $\geq 4.0.0$ $< 4.1.0$ allows anyone with access to the management network to bypass client-certificate based authentication and retrieve information or issue configuration commands via simple HTTP requests to the Agent on port https/9443, because the cmd/agent.py unicorn cert_reqs option is True but is supposed to be ssl.CERT_REQUIRED.

CVE-2019-17134 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.1 - CRITICAL**

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

CVSS2 Score: **6.4 - MEDIUM**

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2019:3788

No Description Provided	Mailing List Patch Third Party Advisory review.opendev.org text/html	 MISC review.opendev.org/686546
Storyboard	Exploit Third Party Advisory storyboard.openstack.org text/html	 MISC storyboard.openstack.org/#!/story/2006660
No Description Provided	Mailing List Patch Third Party Advisory review.opendev.org text/html	 MISC review.opendev.org/686544
USN-4153-1: Octavia vulnerability Ubuntu security notices Ubuntu	Third Party Advisory usn.ubuntu.com text/html	 UBUNTU USN-4153-1
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2020:0721
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2019:3743
OpenStack Docs: OSSA-2019-005: Octavia Amphora-Agent not requiring Client-Certificate	Patch Vendor Advisory security.openstack.org text/html	 CONFIRM security.openstack.org/ossa/OSSA-2019-005.html
No Description Provided	Mailing List Patch Third Party Advisory review.opendev.org text/html	 MISC review.opendev.org/686545
No Description Provided	Mailing List Patch Third Party Advisory review.opendev.org text/html	 MISC review.opendev.org/686547
No Description Provided	Mailing List Patch Third Party Advisory review.opendev.org text/html	 MISC review.opendev.org/686543
No Description Provided	Mailing List Patch Third Party Advisory review.opendev.org text/html	 MISC review.opendev.org/686541

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
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Application	OpenDev	Octavia	All	All	All	All
Application	OpenDev	Octavia	All	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:19.04:*****:*						
cpe:2.3:o:canonical:ubuntu_linux:19.04:*****:*						
cpe:2.3:a:opendev:octavia:*****:openstack:*						
cpe:2.3:a:opendev:octavia:*****:openstack:*						
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](#)