



CVE-2015-3908

Published on: 08/12/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:08 PM UTC

CVE-2015-3908

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Ansible](#) from [Redhat](#) contain the following vulnerability:

Ansible before 1.9.2 does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.

CVE-2015-3908 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

openSUSE-SU-2015:1280-1: moderate: Security update for ansible

[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2015:1280](#)

oss-security - [CVE-2015-3908] Improper TLS Certificate Validation in Ansible

[Mailing List](#)
[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20150714 \[CVE-2015-3908\] Improper TLS Certificate Validation in Ansible](#)

[SECURITY] [DLA 1923-1] ansible security update

[lists.debian.org](#)
[text/html](#)

[MLIST \[debian-lts-announce\] 20190916 \[SECURITY\] \[DLA 1923-1\] ansible security update](#)

openSUSE-SU-2015:1452-1: moderate: Security update for ansible

[Third Party Advisory](#)
[lists.opensuse.org](#)
[text/html](#)

[SUSE openSUSE-SU-2015:1452](#)

Ansible Privacy Policy

[Vendor Advisory](#)
[www.ansible.com](#)

[CONFIRM www.ansible.com/security](#)

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.

Related QID Numbers

980817 Python (pip) Security Update for ansible (GHSA-w64c-pxjj-h866)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible	All	All	All	All
cpe:2.3:a:redhat:ansible:*:*:*:*:*:*:						

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](#)