



CVE-2015-6240

Published on: 06/07/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6240

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

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

The chroot, jail, and zone connection plugins in ansible before 1.9.2 allow local users to escape a restricted environment via a symlink attack.

CVE-2015-6240 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
1243468 – (CVE-2015-3908, CVE-2015-6240) CVE-2015-6240 CVE-2015-3908 ansible: multiple issues fixed in 1.9.2	Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1243468

Fix problem with chroot connection plugins and symlinks from within t... · ansible/ansible@952166f · GitHub

Patch

github.com

text/html

CONFIRM

github.com/ansible/ansible/commit/952166f48eb0f5797b75b160fd156bbe1e8fc647

oss-security - Re: CVE request: ansible zone/chroot/jail escape

Mailing List

Third Party Advisory

www.openwall.com

text/html

MLIST [oss-security] 20150817 Re: CVE request: ansible zone/chroot/jail escape

Fix problem with jail and zone connection plugins and symlinks from w... · ansible/ansible@ca2f2c4 · GitHub

Patch

github.com

text/html

CONFIRM

github.com/ansible/ansible/commit/ca2f2c4ebd7b5e097eab0a710f79c1f63badf95b

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

lists.debian.org

text/html

MLIST [debian-lts-announce] 20190916 [SECURITY] [DLA 1923-1] ansible security update

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	Ansible	All	All	All	All

cpe:2.3:a:redhat:ansible:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →