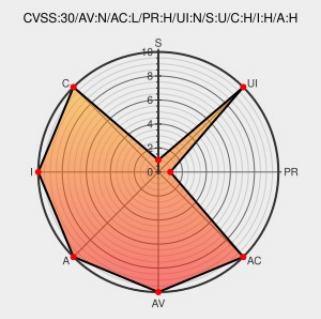
CVE-2017-12148

Published on: 07/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:29 PM UTC

CVE-2017-12148

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



Certain versions of Ansible Tower from Redhat contain the following vulnerability:

A flaw was found in Ansible Tower's interface before 3.1.5 and 3.2.0 with SCM repositories. If a Tower project (SCM repository) definition does not have the 'delete before update' flag set, an attacker with commit access to the upstream playbook source repository could create a Trojan playbook that, when executed by Tower, modifies the checked out SCM repository to add git hooks. These git hooks could, in turn, cause arbitrary command and code execution as the user Tower runs as.

CVE-2017-12148 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Red Hat** - **Ansible Tower** version **3.1.5**

Affected Vendor/Software: **Red Hat** - **Ansible Tower** version **3.2.0**

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
1485474 – (CVE-2017-12148) CVE-2017-12148 Ansible Tower:modification of git hooks in SCM repo via upstream playbook execution	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-12148
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2017:3005

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 Tower	All	All	All	All
Application	Redhat	Ansible Tower	All	All	All	All
Application	Redhat	Ansible Tower	All	All	All	All
Application	Redhat	Ansible Tower	All	All	All	All
Application	Redhat	Cloudforms	4.5	All	All	All
Application	Redhat	Cloudforms	4.5	All	All	All

cpe:2.3:a:redhat:ansible_tower:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_tower:*:*:*:*:scm_repositories:*:*:*:

cpe:2.3:a:redhat:ansible_tower:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_tower:*:*:*:*:scm_repositories:*:*:*:

cpe:2.3:a:redhat:cloudforms:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:cloudforms:4.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report