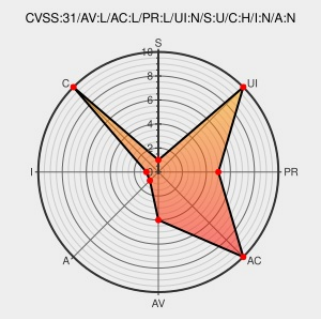
CVE-2019-19341

Published on: 12/19/2019 12:00:00 AM UTC

Last Modified on: 01/31/2023 08:11:00 PM UTC

CVE-2019-19341

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, versions 3.6.x before 3.6.2, where files in '/var/backup/tower' are left world-readable. These files include both the SECRET_KEY and the database backup. Any user with access to the Tower server, and knowledge of when a backup is run, could retrieve every credential stored in Tower. Access to data is the highest threat with this vulnerability.

CVE-2019-19341 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **RedHat** - **Tower** version **all ansible_tower versions 3.6.x before 3.6.2**

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

1782625 – (CVE-2019-19341) CVE-2019-19341 Tower: intermediate files during Tower backup are world-readable	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-19341

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→