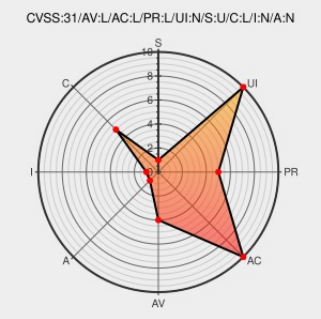
CVE-2020-10698

Published on: 05/27/2021 12:00:00 AM UTC

Last Modified on: 06/15/2022 02:53:00 AM UTC

CVE-2020-10698

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 when running jobs. This flaw allows an attacker to access the stdout of the executed jobs which are run from other organizations. Some sensible data can be disclosed. However, critical data should not be disclosed, as it should be protected by the no_log flag when debugging is enabled. This flaw affects Ansible Tower versions before 3.6.4, Ansible Tower versions before 3.5.6 and Ansible Tower versions before 3.4.6.

CVE-2020-10698 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.3 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	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
1818924 - (CVE-2020-10698) CVE-2020-10698 Tower: normal users can		MISC

1818924 – (CVE-2020-10698) CVE-2020-10698 Tower: normal users can intercept stdout from jobs running in other organizations

bugzilla.redhat.com
text/html

MISC
bugzilla.redhat.com/show_bug.cgi?id=1818924

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-10698 : A flaw was found in Ansible Tower when running jobs. This flaw allows an attacker to access the st… twitter.com/i/web/status/1…	2021-05-27 19:07:52
/r/netcve	CVE-2020-10698	2021-05-27 19:41:31

← 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 registred 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