

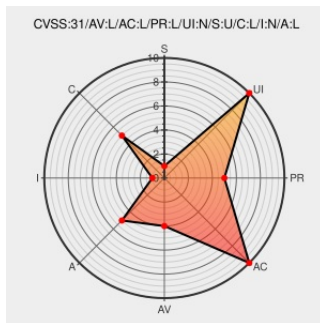


CVE-2020-10697

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

Last Modified on: 10/25/2022 04:10:00 PM UTC

CVE-2020-10697

[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 Openshift. Tower runs a memcached, which is accessed via TCP. An attacker can take advantage of writing a playbook polluting this cache, causing a denial of service attack. This attack would not completely stop the service, but in the worst-case scenario, it can reduce the Tower performance, for which memcached is designed. Theoretically, more sophisticated attacks can be performed by manipulating and crafting the cache, as Tower relies on memcached as a place to pull out setting values. Confidential and sensitive data stored in memcached should not be pulled, as this information is encrypted. 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-2020-10697 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.4 - MEDIUM**

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

CVSS2 Score: **3.6 - LOW**

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

CVE References

Description

1818445 – (CVE-2020-10697) CVE-2020-10697 Tower: memcached deployment is insecure on OpenShift

Tags

bugzilla.redhat.com

text/html

Link

 MISC

bugzilla.redhat.com/show_bug.cgi?id=1818445

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-2020-10697 : A flaw was found in Ansible Tower when running Openshift. Tower runs a memcached, which is accesse... twitter.com/i/web/status/1...	2021-05-27 19:07:37
 /r/netcve	CVE-2020-10697	2021-05-27 19:41:31

← Previous ID

Next ID →