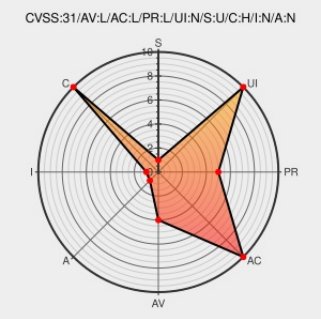
CVE-2020-14327

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

Last Modified on: 06/07/2021 06:41:00 PM UTC

CVE-2020-14327

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



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

A Server-side request forgery (SSRF) flaw was found in Ansible Tower in versions before 3.6.5 and before 3.7.2. Functionality on the Tower server is abused by supplying a URL that could lead to the server processing it. This flaw leads to the connection to internal services or the exposure of additional internal services by abusing the test feature of lookup credentials to forge HTTP/HTTPS requests from the server and retrieving the results of the response.

CVE-2020-14327 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

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
1856785 - (CVE-2020-14327) CVE-2020-14327 Tower: SSRF: Server Side		MISC

1856785 – (CVE-2020-14327) CVE-2020-14327 Tower: SSRF: Server Side Request Forgery on Credential	bugzilla.redhat.com text/html	MISC	bugzilla.redhat.com/show_bug.cgi?id=1856785

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for exploiting CVE-2020-14327

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-2020-14327 : A Server-side request forgery #SSRF flaw was found in Ansible Tower in versions before 3.6.5 and… twitter.com/i/web/status/1…	2021-05-27 20:04:56
/r/netcve	CVE-2020-14327	2021-05-27 20:41:38

← Previous ID

Next ID→