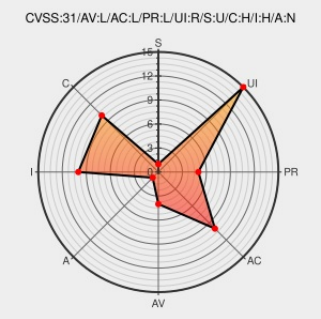
CVE-2021-3701

Published on: Not Yet Published

Last Modified on: 02/17/2023 07:06:00 PM UTC

CVE-2021-3701

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



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

A flaw was found in ansible-runner where the default temporary files configuration in ansible-2.0.0 are written to world R/W locations. This flaw allows an attacker to pre-create the directory, resulting in reading private information or forcing ansible-runner to write files as the legitimate user in a place they did not expect. The highest threat from this vulnerability is to confidentiality and integrity.

CVE-2021-3701 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.6 - MEDIUM

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

CVE References

Description	Tags	Link
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2021-3701
1977959 – (CVE-2021-3701) CVE-2021-3701 ansible-runner: Artifacts are written to world rw location by default	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1977959
Secure tempfiles by abadger · Pull Request #742 · ansible/ansible-runner · GitHub	github.com text/html	MISC github.com/ansible/ansible-runner/pull/742/commits
ansible-runner writes artifacts to world rw location by default · Issue #738 · ansible/ansible-runner · GitHub	github.com text/html	MISC github.com/ansible/ansible-runner/issues/738

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.

Related QID Numbers

184510 Debian Security Update for ansible-runner (CVE-2021-3701)

Exploit/POC from Github

A flaw was found in ansible-runner where the default temporary files configuration in ansible-2.0.0 are written to wo…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible Runner	2.0.0	-	All	All

cpe:2.3:a:redhat:ansible_runner:2.0.0:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-3701 : A flaw was found in ansible-runner where the default temporary files configuration in ansible-2.0.0… twitter.com/i/web/status/1…	2022-08-23 16:12:17
@LinInfoSec	Ansible - CVE-2021-3701: access.redhat.com/security/cve/C…	2022-08-23 19:02:28
/r/netcve	CVE-2021-3701	2022-08-23 17:39:00

← Previous ID Next ID→