

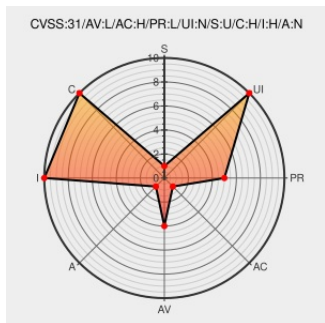


CVE-2021-3702

Published on: Not Yet Published

Last Modified on: 02/12/2023 11:07:00 PM UTC

CVE-2021-3702

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Ansible Runner](#) from [Redhat](#) contain the following vulnerability:

A race condition flaw was found in ansible-runner, where an attacker could watch for rapid creation and deletion of a temporary directory, substitute their directory at that name, and then have access to ansible-runner's private_data_dir the next time ansible-runner made use of the private_data_dir. The highest Threat out of this flaw is to

integrity and confidentiality.

CVE-2021-3702 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Secure tempfiles by abadger · Pull Request #742 · ansible/ansible-runner · GitHub	github.com text/html	MISC github.com/ansible/ansible-runner/pull/742/commits
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2021-3702
1977965 – (CVE-2021-3702) CVE-2021-3702 ansible-runner: Race condition with temporary files in tempfile.TemporaryDirectory()	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1977965

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

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 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-2021-3702 : A race condition flaw was found in ansible-runner, where an attacker could watch for rapid creation... twitter.com/i/web/status/1...	2022-08-23 16:12:31
 @LinInfoSec	Ansible - CVE-2021-3702: bugzilla.redhat.com/show_bug.cgi?i...	2022-08-23 19:02:28
 /r/netcve	CVE-2021-3702	2022-08-23 17:39:01

[← 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 registered 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](#)