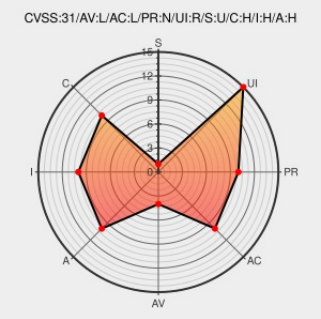
CVE-2021-4041

Published on: Not Yet Published

Last Modified on: 08/29/2022 02:30:00 PM UTC

CVE-2021-4041

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. An improper escaping of the shell command, while calling the ansible_runner.interface.run_command, can lead to parameters getting executed as host's shell command. A developer could unintentionally write code that gets executed in the host rather than the virtual environment.

CVE-2021-4041 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
2028074 – (CVE-2021-4041) CVE-2021-4041 Ansible: Improper shell escaping in ansible-runner	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=2028074
Red Hat Customer Portal - Access to 24x7 support and knowledge	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2021-4041
Remove shell use in subprocess · ansible/ansible-runner@3533f26 · GitHub	github.com text/html	MISC github.com/ansible/ansible-runner/commit/3533f265f4349a3f2a0283158cd01b59a6bbc7bd

Related QID Numbers

183895 Debian Security Update for ansible-runner (CVE-2021-4041)

Exploit/POC from Github

A flaw was found in ansible-runner. An improper escaping of the shell command, while calling the ansible_runner.inter…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible Runner	All	All	All	All
Application	Redhat	Ansible Runner	2.1.0	alpha1	All	All
Application	Redhat	Ansible Runner	2.1.0	alpha2	All	All
Application	Redhat	Ansible Runner	2.1.0	beta1	All	All

cpe:2.3:a:redhat:ansible_runner:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_runner:2.1.0:alpha1:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_runner:2.1.0:alpha2:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_runner:2.1.0:beta1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-4041 : A flaw was found in ansible-runner. An improper escaping of the shell command, while calling the… twitter.com/i/web/status/1…	2022-08-24 16:09:17
@LinInfoSec	Ansible - CVE-2021-4041: bugzilla.redhat.com/show_bug.cgi?i…	2022-08-24 19:00:39
/r/netcve	CVE-2021-4041	2022-08-24 17:38:53

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report