



# CVE-2021-3583

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2021-3583
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-09-22 12:15:00 UTC
<b>Updated</b>	2023-12-28 19:15:00 UTC
<b>Description</b>	A flaw was found in Ansible, where a user's controller is vulnerable to template injection. This issue can occur through facts

## Risk And Classification

**Problem Types:** CWE-94

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Redhat</a>	<a href="#">Ansible Automation Platform</a>	1.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible Engine</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	All	All	All	All

## References

### Reference

- [SECURITY] [DLA 3695-1] ansible security update
- 1968412 – (CVE-2021-3583) CVE-2021-3583 ansible: Template Injection through yaml multi-line strings with ansible facts used in template.
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[182514](#) Debian Security Update for ansibleansible-core (CVE-2021-3583)

[239484](#) Red Hat Update for Ansible (RHSA-2021:2664)

[2021-09-22](#) Debian Security Update for ansibleansible-core (CVE-2021-3583)

<a href="#">239485</a> Red Hat Update for Ansible (RHSA-2021:2663)
<a href="#">281674</a> Fedora Security Update for ansible (FEDORA-2021-574ee4dd30)
<a href="#">281675</a> Fedora Security Update for ansible (FEDORA-2021-4ad7c70d71)
<a href="#">356238</a> Amazon Linux Security Advisory for ansible : ALASANSIBLE2-2023-001
<a href="#">356502</a> Amazon Linux Security Advisory for ansible : ALAS2ANSIBLE2-2023-001
<a href="#">6000405</a> Debian Security Update for ansible (DLA 3695-1)
<a href="#">690099</a> Free Berkeley Software Distribution (FreeBSD) Security Update for ansible (4c9159ea-d4c9-11eb-aaaa-8c164582fbac)
<a href="#">752570</a> SUSE Enterprise Linux Important for SUSE Manager Client Tools (SUSE-SU-2022:3178-1)
<a href="#">900417</a> Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (6009)
<a href="#">900897</a> Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (6305-1)
<a href="#">980519</a> Python (pip) Security Update for ansible (GHSA-2pfh-q76x-gwvm)

© [CVE.report](#) 2026 |

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](#)**