CVE-2021-3583

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-3583
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-22 12:15:00 UTC
Updated	2023-12-28 19:15:00 UTC
Description	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	Redhat	Ansible Automation Platform	1.2	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Ansible Tower	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)

239485 Red Hat Update for Ansible (RHSA-2021:2663)

281674 Fedora Security Update for ansible (FEDORA-2021-574ee4dd30)

281675 Fedora Security Update for ansible (FEDORA-2021-4ad7c70d71)

356238 Amazon Linux Security Advisory for ansible : ALASANSIBLE2-2023-001

356502 Amazon Linux Security Advisory for ansible : ALAS2ANSIBLE2-2023-001

6000405 Debian Security Update for ansible (DLA 3695-1)

690099 Free Berkeley Software Distribution (FreeBSD) Security Update for ansible (4c9159ea-d4c9-11eb-aeee-8c164582fbac)

752570 SUSE Enterprise Linux Important for SUSE Manager Client Tools (SUSE-SU-2022:3178-1)

900417 Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (6009)

900897 Common Base Linux Mariner (CBL-Mariner) Security Update for ansible (6305-1)

980519 Python (pip) Security Update for ansible (GHSA-2pfh-q76x-gwvm)