



CVE-2020-14365

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

Summary

CVE	CVE-2020-14365
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-23 13:15:00 UTC
Updated	2022-04-05 15:29:00 UTC
Description	A flaw was found in the Ansible Engine, in ansible-engine 2.8.x before 2.8.15 and ansible-engine 2.9.x before 2.9.13, when

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Ansible Tower	3.0	All	All	All
Application	Redhat	Ansible Tower	3.0	All	All	All
Application	Redhat	Ansible Tower	All	All	All	All
Application	Redhat	Ansible Tower	All	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	3.0	All	All	All
Application	Redhat	Ceph Storage	2.0	All	All	All
Application	Redhat	Ceph Storage	3.0	All	All	All
Application	Redhat	Openstack Platform	10.0	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All
Application	Redhat	Openstack Platform	10.0	All	All	All
Application	Redhat	Openstack Platform	13.0	All	All	All

References

Reference	Source	Link
1869154 – (CVE-2020-14365) CVE-2020-14365 ansible: dnf module install packages with no GPG signature	MISC	bugzilla.redhat.c
Debian -- Security Information -- DSA-4950-1 ansible	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [178744](#) Debian Security Update for ansible (DSA 4950-1)
- [356179](#) Amazon Linux Security Advisory for ansible : ALASANSIBLE2-2023-005
- [375885](#) Ansible Engine Arbitrary Code Execution Vulnerability
- [500006](#) Alpine Linux Security Update for ansible
- [501347](#) Alpine Linux Security Update for ansible-base
- [981388](#) Python (pip) Security Update for ansible (GHSA-m429-fhmv-c6q2)

© [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](#)