



CVE-2020-10691

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

Summary

CVE	CVE-2020-10691
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-30 17:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	An archive traversal flaw was found in all ansible-engine versions 2.9.x prior to 2.9.7, when running ansible-galaxy collectio

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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

References

Reference
ansible-galaxy - Fix tar path traversal issue during install - CVE-2020-10691 by jborean93 · Pull Request #68596 · ansible/ansible · GitHub
1817161 – (CVE-2020-10691) CVE-2020-10691 Ansible: archive traversal vulnerability in ansible-galaxy collection install
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

356226 Amazon Linux Security Advisory for ansible : ALASANSIBLE2-2023-008
500010 Alpine Linux Security Update for ansible

501350 Alpine Linux Security Update for ansible-base

982729 Python (pip) Security Update for ansible (GHSA-3c67-gc48-983w)

© [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](#)