



CVE-2022-3697

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

Summary

CVE	CVE-2022-3697
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-28 16:15:00 UTC
Updated	2023-12-28 19:15:00 UTC
Description	A flaw was found in Ansible in the amazon.aws collection when using the tower_callback parameter from the amazon.aws.c

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible	All	All	All	All
Application	Redhat	Ansible Collection	All	All	All	All
Application	Redhat	Ansible Collection	All	All	All	All

References

Reference	Source
[SECURITY] [DLA 3695-1] ansible security update	
ec2_instance - validate options on tower_callback by tremble · Pull Request #1199 · ansible-collections/amazon.aws · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184266 Debian Security Update for ansible (CVE-2022-3697)

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

001107 C... .. (CPE 2.3) (DLA 3695-1)

© [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](#)