



CVE-2018-10884

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

Summary

CVE	CVE-2018-10884
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-22 14:29:00 UTC
Updated	2019-10-09 23:33:00 UTC
Description	Ansible Tower before versions 3.1.8 and 3.2.6 is vulnerable to cross-site request forgery (CSRF) in awx/api/authentication.p

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference

Malformed Request

1597069 – (CVE-2018-10884) CVE-2018-10884 ansible-tower: CSRF in awx/api/authentication.py allows for hijacking of the authtoken cookie

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report