



# CVE-2019-14864

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

## Summary

<b>CVE</b>	CVE-2019-14864
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-02 15:15:00 UTC
<b>Updated</b>	2022-04-22 19:59:00 UTC
<b>Description</b>	Ansible, versions 2.9.x before 2.9.1, 2.8.x before 2.8.7 and Ansible versions 2.7.x before 2.7.15, is not respecting the flag n

## Risk And Classification

**Problem Types:** CWE-532 | CWE-117

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Application	<a href="#">Opensuse</a>	<a href="#">Backports Sle</a>	15.0	sp1	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible</a>	All	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ansible Tower</a>	3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ceph Storage</a>	3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Ceph Storage</a>	3.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Cloudforms Management Engine</a>	5.0	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Cloudforms Management Engine</a>	5.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All

## References

Reference	Source
Sumologic callback plugin logging sensitive data · Issue #63522 · ansible/ansible · GitHub	MISC
[security-announce] openSUSE-SU-2020:0513-1: moderate: Security update f	SUSE
[security-announce] openSUSE-SU-2020:0523-1: moderate: Security update f	SUSE
1764148 – (CVE-2019-14864) CVE-2019-14864 Ansible: Splunk and Sumologic callback plugins leak sensitive data in logs	CONFIR
removing args from task_fields as it can contain sensitive data by poblahblahblah · Pull Request #63527 · ansible/ansible · GitHub	MISC
Debian -- Security Information -- DSA-4950-1 ansible	DEBIAN
CVE Program record	CVE.OR
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 178744 Debian Security Update for ansible (DSA 4950-1)
- 981585 Python (pip) Security Update for ansible (GHSA-3m93-m4q6-mc6v)

© 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](#)**