



# CVE-2019-14846

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

## Summary

<b>CVE</b>	CVE-2019-14846
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-10-08 19:15:00 UTC
<b>Updated</b>	2022-04-22 19:56:00 UTC
<b>Description</b>	In Ansible, all Ansible Engine versions up to ansible-engine 2.8.5, ansible-engine 2.7.13, ansible-engine 2.6.19, were logging

## 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	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Ansible Engine	2.0	All	All	All
Application	Redhat	Ansible Engine	2.6.0	All	All	All
Application	Redhat	Ansible Engine	2.7.0	All	All	All
Application	Redhat	Ansible Engine	2.8.0	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Ansible Engine	2.0	All	All	All
Application	Redhat	Ansible Engine	2.6.0	All	All	All

Application	Redhat	Ansible Engine	2.7.0	All	All	All
Application	Redhat	Ansible Engine	2.8.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	8.0	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	13.0	All	All	All

## References

Reference	Source
Red Hat Customer Portal	REDHAT
[SECURITY] [DLA 2202-1] ansible security update	MLIST
[security-announce] openSUSE-SU-2020:0513-1: moderate: Security update f	SUSE
Fix for plugins which used the boto libraries leaking the boto creden... by abadger · Pull Request #63366 · ansible/ansible · GitHub	CONFIR
[security-announce] openSUSE-SU-2020:0523-1: moderate: Security update f	SUSE
[SECURITY] [DLA 2535-1] ansible security update	MLIST
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
1755373 – (CVE-2019-14846) CVE-2019-14846 ansible: secrets disclosed on logs when no_log enabled	CONFIR
Debian -- Security Information -- DSA-4950-1 ansible	DEBIAN
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
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)

[500006](#) Alpine Linux Security Update for ansible

[501346](#) Alpine Linux Security Update for ansible-base

© [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](#)**