CVE-2018-16876

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2018-16876
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-03 15:29:00 UTC
Updated	2021-08-04 17:15:00 UTC
Description	ansible before versions 2.5.14, 2.6.11, 2.7.5 is vulnerable to a information disclosure flaw in vvv+ mode with no_log on that

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Redhat	Ansible	All	All	All	All
Application	Redhat	Ansible	All	All	All	All
Application	Redhat	Ansible Engine	2.0	All	All	All
Application	Redhat	Ansible Engine	2.5	All	All	All
Application	Redhat	Ansible Engine	2.6	All	All	All
Application	Redhat	Ansible Engine	2.7	All	All	All
Application	Redhat	Ansible Engine	2.0	All	All	All
Application	Redhat	Ansible Engine	2.5	All	All	All
Application	Redhat	Ansible Engine	2.6	All	All	All

Application	Redhat	Ansible Engine	2.7	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Redhat	Openstack	14	All	All	All
Application	Redhat	Openstack	14.0	All	All	All
Application	Redhat	Openstack	14.0	All	All	All
Operating System	Suse	Linux Enterprise	12.0	All	All	All
Operating System	Suse	Linux Enterprise	12.0	All	All	All
Application	Suse	Package Hub	-	All	All	All
Application	Suse	Package Hub	-	All	All	All

References

Reference	Source	Link
ensure ssh retry respects no log by bcoca · Pull Request #49569 · ansible/ansible · GitHub	MISC	github.com
Red Hat Customer Portal	REDHAT	access.redhat.co
Red Hat Customer Portal	REDHAT	access.redhat.co
[security-announce] openSUSE-SU-2019:1858-1: moderate: Security update f	SUSE	lists.opensuse.or
[security-announce] openSUSE-SU-2019:1635-1: moderate: Security update f	SUSE	lists.opensuse.or
Red Hat Customer Portal	REDHAT	access.redhat.co
Red Hat Customer Portal	REDHAT	access.redhat.co
1657330 – (CVE-2018-16876) CVE-2018-16876 ansible: Information disclosure in vvv+ mode with no_log on	CONFIRM	bugzilla.redhat.c
Red Hat Customer Portal	REDHAT	access.redhat.co
USN-4072-1: Ansible vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal	REDHAT	access.redhat.co
Debian -- Security Information -- DSA-4396-1 ansible	DEBIAN	www.debian.org
[security-announce] openSUSE-SU-2019:1125-1: moderate: Security update f	SUSE	lists.opensuse.or
Ansible CVE-2018-16876 Remote Information Disclosure Vulnerability	BID	www.securityfocu
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500002 Alpine Linux Security Update for ansible

501343 Alpine Linux Security Update for ansible-base

Free CVE JSON API cve.report/api

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