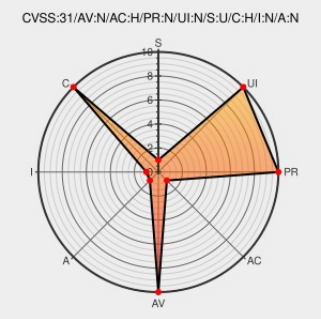
CVE-2018-10855

Published on: 07/02/2018 12:00:00 AM UTC

Last Modified on: 08/04/2021 05:14:00 PM UTC

CVE-2018-10855

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Ansible 2.5 prior to 2.5.5, and 2.4 prior to 2.4.5, do not honor the no_log task flag for failed tasks. When the no_log flag has been used to protect sensitive data passed to a task from being logged, and that task does not run successfully, Ansible will expose sensitive data in log files and on the terminal of the user running Ansible.

CVE-2018-10855 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **[UNKNOWN]** - **ansible** version **Ansible 2.4.5**

Affected Vendor/Software: **[UNKNOWN]** - **ansible** version **Ansible 2.5.5**

CVSS3 Score: 5.9 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link

Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2022
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHBA-2018:3788
USN-4072-1: Ansible vulnerabilities | Ubuntu security notices	Third Party Advisory usn.ubuntu.com text/html	UBUNTU USN-4072-1
Debian -- Security Information -- DSA-4396-1 ansible	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4396
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:1949
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2585
1588855 – (CVE-2018-10855) CVE-2018-10855 ansible: Failed tasks do not honour no_log option allowing for secrets to be disclosed in logs	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10855
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:1948
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2184
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:0054
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2079

Related QID Numbers

981353 Python (pip) Security Update for ansible (GHSA-jwcc-j78w-j73w)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating	Canonical	Ubuntu Linux	18.04	All	All	All

System						
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 Engine	All	All	All	All
Application	Redhat	Ansible Engine	2.0	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Ansible Engine	2.0	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Cloudforms	4.6	All	All	All
Application	Redhat	Cloudforms	4.6	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	12	All	All	All
Application	Redhat	Openstack	13	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	12	All	All	All
Application	Redhat	Openstack	13.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All
Application	Redhat	Virtualization	4.0	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:16.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:18.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:19.04:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:ansible_engine:*:*:*:*:*:*:*:*

cpe:2.3:a:redhat:ansible_engine:2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:ansible_engine:*:*:*:*:*:*:*:*

cpe:2.3:a:redhat:ansible_engine:2.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:ansible_engine:*:*:*:*:*:*:*:*

cpe:2.3:a:redhat:cloudforms:4.6:*:*:*:*:*:*:*

cpe:2.3:a:redhat:cloudforms:4.6:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openstack:10:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openstack:12:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openstack:13:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openstack:13.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openstack:10:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openstack:12:*:*:*:*:*:*:*

cpe:2.3:a:redhat:openstack:13.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:virtualization:4.0:*:*:*:*:*:*:*

cpe:2.3:a:redhat:virtualization:4.0:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→