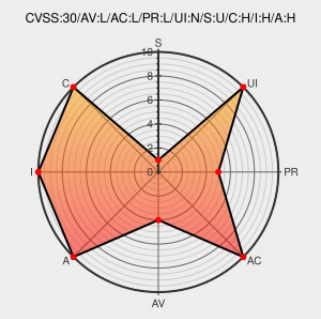
CVE-2018-10874

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

Last Modified on: 02/13/2023 04:51:00 AM UTC

CVE-2018-10874

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



Certain versions of Ansible Engine from Redhat contain the following vulnerability:

In ansible it was found that inventory variables are loaded from current working directory when running ad-hoc command which are under attacker's control, allowing to run arbitrary code as a result.

CVE-2018-10874 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **[UNKNOWN]** - **ansible** version **= n/a**

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2150

1596528 – (CVE-2018-10874) CVE-2018-10874 ansible: Inventory variables are loaded from current working directory when running ad-hoc command that can lead to code execution	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10874
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2152
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2151
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHBA-2018:3788
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2166
CVE-2018-10874 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2018-10874
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2321
USN-4072-1: Ansible vulnerabilities | Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-4072-1
Red Hat Enterprise Virtualization Bugs in Ansible Component Lets Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041396
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2018:2585
1596528 – (CVE-2018-10874) CVE-2018-10874 ansible: Inventory variables are loaded from current working directory when running ad-hoc command that can lead to code execution	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1596528
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2019:0054

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible Engine	2.0	All	All	All
Application	Redhat	Ansible Engine	2.4	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	2.0	All	All	All
Application	Redhat	Ansible Engine	2.4	All	All	All
Application	Redhat	Ansible Engine	2.5	All	All	All
Application	Redhat	Ansible Engine	2.6	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
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

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

cpe:2.3:a:redhat:ansible_engine:2.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_engine:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_engine:2.6:*:*:*:*:*:*:*:

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

cpe:2.3:a:redhat:ansible_engine:2.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_engine:2.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible_engine:2.6:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:virtualization_host:4.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→