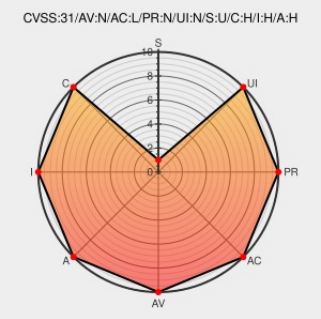
CVE-2014-4966

Published on: 02/18/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:44 PM UTC

CVE-2014-4966

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



Certain versions of Ansible from Redhat contain the following vulnerability:

Ansible before 1.6.7 does not prevent inventory data with "{{" and "lookup" substrings, and does not prevent remote data with "{{" substrings, which allows remote attackers to execute arbitrary code via (1) crafted lookup('pipe') calls or (2) crafted Jinja2 data.

CVE-2014-4966 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
oCERT.org - oCERT Advisories	Third Party Advisory, www.ocert.org, text/xml	MISC www.ocert.org/advisories/ocert-2014-004.html
Security fixes: ·	Patch	CONFIRM

ansible/ansible@62a1295 · GitHub	Third Party Advisory github.com text/html	github.com/ansible/ansible/commit/62a1295a3e08cb6c3e9f1b2a1e6e5dcaeab32527

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	All	All	All	All
Application	Redhat	Ansible	All	All	All	All

cpe:2.3:a:redhat:ansible:*:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:ansible:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→