



CVE-2014-4657

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

Summary

CVE	CVE-2014-4657
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-20 15:15:00 UTC
Updated	2020-02-25 21:14:00 UTC
Description	The safe_eval function in Ansible before 1.5.4 does not properly restrict the code subset, which allows remote attackers to e

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Ansible	All	All	All	All
Application	Redhat	Ansible	All	All	All	All

References

Reference	Source	Link	Tags
Ansible CVE-2014-4657 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
ansible/CHANGELOG.md at release1.5.5 · ansible/ansible · GitHub	CONFIRM	github.com	Release Notes
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[994801](#) Python (Pip) Security Update for ansible (GHSA-qg47-5px9-32g7)

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](#).

Free CVE JSON API cve.report/api

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