CVE-2016-9587

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

Summary

CVE	CVE-2016-9587
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-24 16:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	Ansible before versions 2.1.4, 2.2.1 is vulnerable to an improper input validation in Ansible's handling of data sent from clier

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ansible	Ansible	All	All	All	All
Application	Ansible	Ansible	All	All	All	All
Application	Redhat	Ansible	All	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	11.0	All	All	All

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
Ansible: Remote execution of arbitrary code (GLSA 201701-77) — Gentoo Security
Red Hat Customer Portal
Ansible 2.1.4/2.2.1 - Command Execution - Linux remote Exploit
Red Hat Customer Portal
1404378 – (CVE-2016-9587) CVE-2016-9587 Ansible: Compromised remote hosts can lead to running commands on the Ansible controller
Ansible CVE-2016-9587 Arbitrary Command Execution Vulnerability

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981352 Python (pip) Security Update for ansible (GHSA-m956-frf4-m2wr)