CVE-2017-7466

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

Summary

CVE	CVE-2017-7466
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-22 13:29:00 UTC
Updated	2021-08-04 17:15:00 UTC
Description	Ansible before version 2.3 has an input validation vulnerability in the handling of data sent from client systems. An attacker

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
Application	Redhat	Openstack	10	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	11	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	11.0	All	All	All

References

Reference	Source
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
1439212 – (CVE-2017-7466) CVE-2017-7466 ansible: Arbitrary code execution on control node (incomplete fix for CVE-2016-9587)	CONFI
Ansible CVE-2017-7466 Incomplete Fix Arbitrary Command Execution Vulnerability	BID
Red Hat Customer Portal	REDHA

Red Hat Customer Portal	REDHA
Red Hat Customer Portal	REDHA
CVE Program record	CVE.O
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.