



CVE-2017-7481

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

Summary

CVE	CVE-2017-7481
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-19 13:29:00 UTC
Updated	2021-08-04 17:15:00 UTC
Description	Ansible before versions 2.3.1.0 and 2.4.0.0 fails to properly mark lookup-plugin results as unsafe. If an attacker could contr

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Application	Redhat	Ansible Engine	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Gluster Storage	3.2	All	All	All
Application	Redhat	Gluster Storage	3.2	All	All	All
Application	Redhat	Openshift Container Platform	3.3	All	All	All
Application	Redhat	Openshift Container Platform	3.4	All	All	All
Application	Redhat	Openshift Container Platform	3.5	All	All	All

Application	Redhat	Openshift Container Platform	3.3	All	All	All
Application	Redhat	Openshift Container Platform	3.4	All	All	All
Application	Redhat	Openshift Container Platform	3.5	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
Application	Redhat	Storage Console	2.0	All	All	All
Application	Redhat	Storage Console	2.0	All	All	All
Application	Redhat	Virtualization	4.1	All	All	All
Application	Redhat	Virtualization	4.1	All	All	All
Application	Redhat	Virtualization Manager	4.1	All	All	All
Application	Redhat	Virtualization Manager	4.1	All	All	All

References				
Reference	Source	Link		
Red Hat Customer Portal	REDHAT	access		
Red Hat Customer Portal	REDHAT	access		
Red Hat Customer Portal	REDHAT	access		
[SECURITY] [DLA 2535-1] ansible security update	MLIST	lists		
USN-4072-1: Ansible vulnerabilities Ubuntu security notices	UBUNTU	usn		
1450018 – (CVE-2017-7481) CVE-2017-7481 ansible: Security issue with lookup return not tainting the jinja2 environment	CONFIRM	bug		
Red Hat Customer Portal	REDHAT	access		
Red Hat Customer Portal	REDHAT	access		
Red Hat Customer Portal	REDHAT	access		
Ansible CVE-2017-7481 Security Bypass Vulnerability	BID	www		
Fixing security issue with lookup returns not tainting the jinja2 env... · ansible/ansible@ed56f51 · GitHub	CONFIRM	gith		
CVE Program record	CVE.ORG	ww		
NVD vulnerability detail	NVD	nvd		

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)