CVE-2017-7549

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

Summary

CVE	CVE-2017-7549
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-21 21:29:00 UTC
Updated	2023-02-12 23:31:00 UTC
Description	A flaw was found in instack-undercloud 7.2.0 as packaged in Red Hat OpenStack Platform Pike, 6.1.0 as packaged in Red

Risk And Classification

Problem Types: CWE-377

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Instack-undercloud	5.3.0	All	All	All
Application	Openstack	Instack-undercloud	6.1.0	All	All	All
Application	Openstack	Instack-undercloud	7.2.0	All	All	All
Application	Openstack	Instack-undercloud	5.3.0	All	All	All
Application	Openstack	Instack-undercloud	6.1.0	All	All	All
Application	Openstack	Instack-undercloud	7.2.0	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	12	All	All	All
Application	Redhat	Openstack	12.0	All	All	All
Application	Redhat	Openstack	10.0	All	All	All
Application	Redhat	Openstack	11.0	All	All	All
Application	Redhat	Openstack	12.0	All	All	All

References

Reference	Source	Link	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	
1477403 – (CVE-2017-7549) CVE-2017-7549 instack-undercloud: uses hardcoded /tmp paths	CONFIRM	bugzilla.redhat.com	Issue
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Openstack instack-undercloud CVE-2017-7549 Insecure Temporary File Handling Vulnerability	BID	www.securityfocus.com	Third
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
CVE-2017-7549 - Red Hat Customer Portal	MISC	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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