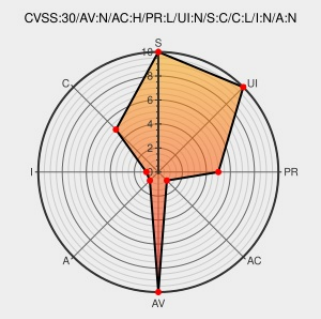
CVE-2015-7548

Published on: 01/12/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:12:03 PM UTC

CVE-2015-7548

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Nova from Openstack contain the following vulnerability:

OpenStack Compute (Nova) before 2015.1.3 (kilo) and 12.0.x before 12.0.1 (liberty), when using libvirt to spawn instances and use_cow_images is set to false, allow remote authenticated users to read arbitrary files by overwriting an instance disk with a crafted image and requesting a snapshot.

CVE-2015-7548 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.5 - LOW

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	NONE	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html	REDHAT RHSA-2016:0018

	Inactive Link Not Archived	
OpenStack Compute (Nova) 'imagebackend.py' Incomplete Fix Information Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 80176
OSSA-2016-001: Nova host data leak through snapshot — OpenStack Security Advisories 2014.2.0.dev125 documentation	Vendor Advisory security.openstack.org text/html	CONFIRM security.openstack.org/ossa/OSSA-2016-001.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Nova	All	All	All	All
Application	Openstack	Nova	All	All	All	All

cpe:2.3:a:openstack:nova:*:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:nova:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→