



CVE-2015-8749

Published on: 01/15/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

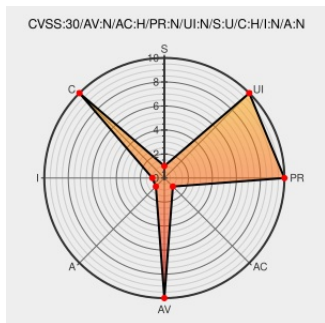
CVE-2015-8749

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Nova](#) from [Openstack](#) contain the following vulnerability:

The `volume_utils._parse_volume_info` function in OpenStack Compute (Nova) before 2015.1.3 (kilo) and 12.0.x before 12.0.1 (liberty) includes the `connection_info` dictionary in the `StorageError` message when using the Xen backend, which might allow attackers to obtain sensitive password information by reading log files or other unspecified vectors.

CVE-2015-8749 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.9 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
oss-security - CVE request for vulnerability in OpenStack Nova	Mailing List Third Party Advisory www.openwall.com	MLIST [oss-security] 20160107 CVE request for vulnerability in OpenStack Nova

	text/html	
Bug #1516765 "[OSSA 2016-002] xenapi: volume_utils._parse_volume..." : Bugs : OpenStack Compute (nova)	Third Party Advisory bugs.launchpad.net text/html	 CONFIRM bugs.launchpad.net/nova/+bug/1516765
OpenStack Nova CVE-2015-8749 Information Disclosure Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 80189
OSSA-2016-002: Xen connection password leak in logs via StorageError — OpenStack Security Advisories 2014.2.0.dev124 documentation	Patch Vendor Advisory security.openstack.org text/html	 CONFIRM security.openstack.org/ossa/OSSA-2016-002.html
oss-security - Re: CVE request for vulnerability in OpenStack Nova	Mailing List Third Party Advisory www.openwall.com text/html	 MLIST [oss-security] 20160107 Re: CVE request for vulnerability in OpenStack Nova

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)