



CVE-2016-4911

Published on: 06/13/2016 12:00:00 AM UTC

Last Modified on: 07/23/2022 10:22:00 AM UTC

CVE-2016-4911

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The Fernet Token Provider in OpenStack Identity (Keystone) 9.0.x before 9.0.1 (mitaka) allows remote authenticated users to prevent revocation of a chain of tokens and bypass intended access restrictions by rescoping a token.

CVE-2016-4911 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
OpenStack Keystone CVE-2016-4911 Security Bypass Vulnerability	cve.report (archive) text/html	🌐 BID 90728
oss-security - Re: CVE request for vulnerability in OpenStack Keystone	www.openwall.com text/html	🔗 MLIST [oss-security] 20160517 Re: CVE request for vulnerability in OpenStack

Gerrit Code Review	review.openstack.org text/html	 CONFIRM review.openstack.org/#/c/311886/
Bug #1577558 "[OSSA 2016-008] v2.0 fernet tokens audit ids are i..." : Bugs : OpenStack Identity (keystone)	bugs.launchpad.net text/html	 CONFIRM bugs.launchpad.net/keystone/+bug/1577558
OSSA-2016-008: Incorrect Audit IDs in Keystone Fernet Tokens can result in revocation bypass — OpenStack Security Advisories 2014.2.0.dev134 documentation	Patch Vendor Advisory security.openstack.org text/html	 CONFIRM security.openstack.org/ossa/OSSA-2016-008.html
oss-security - CVE request for vulnerability in OpenStack Keystone	www.openwall.com text/html	 MLIST [oss-security] 20160517 CVE request for vulnerability in OpenStack Keystone

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	Keystone	Openstack Identity	9.0.0.0	rc1	All	All
Application	Keystone	Openstack Identity	9.0.0.0	rc2	All	All
Application	Keystone	Openstack Identity	9.0.0.0	rc3	All	All
Application	Openstack Project	Openstack Identity	9.0.0.0	rc1	All	All
Application	Openstack Project	Openstack Identity	9.0.0.0	rc2	All	All
Application	Openstack Project	Openstack Identity	9.0.0.0	rc3	All	All
Application	Openstack Project	Openstack Identity	9.0.0.0	rc1	All	All
Application	Openstack Project	Openstack Identity	9.0.0.0	rc2	All	All
Application	Openstack Project	Openstack Identity	9.0.0.0	rc3	All	All
cpe:2.3:a:keystone:openstack_identity:9.0.0.0:rc1:*:*:*:*:*:						
cpe:2.3:a:keystone:openstack_identity:9.0.0.0:rc2:*:*:*:*:*:						
cpe:2.3:a:keystone:openstack_identity:9.0.0.0:rc3:*:*:*:*:*:						
cpe:2.3:a:openstack_project:openstack_identity:9.0.0.0:rc1:*:*:*:*:*:						
cpe:2.3:a:openstack_project:openstack_identity:9.0.0.0:rc2:*:*:*:*:*:						
cpe:2.3:a:openstack_project:openstack_identity:9.0.0.0:rc3:*:*:*:*:*:						
cpe:2.3:a:openstack_project:openstack_identity:9.0.0.0:rc1:*:*:*:*:*:						
cpe:2.3:a:openstack_project:openstack_identity:9.0.0.0:rc2:*:*:*:*:*:						

cpe:2.3:a:openstack_project:openstack_identity:9.0.0.0:rc3:*****:

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](#)