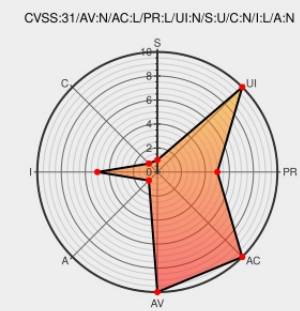
CVE-2016-4911

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 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

		Keystone
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

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→