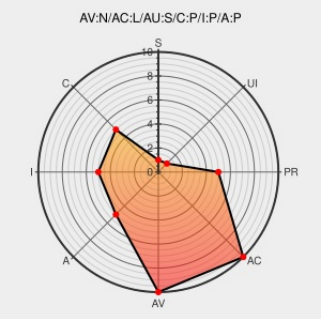
CVE-2014-3520

Published on: 10/26/2014 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:40:00 AM UTC

CVE-2014-3520

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



Certain versions of Keystone from Openstack contain the following vulnerability:

OpenStack Identity (Keystone) before 2013.2.4, 2014.x before 2014.1.2, and Juno before Juno-2 allows remote authenticated trustees to gain access to an unauthorized project for which the trustor has certain roles via the project ID in a V2 API trust token request.

CVE-2014-3520 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
access.redhat.com | CVE-2014-3520	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2014-3520
Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/errata/RHSA-2014:0994
OpenStack Open Source Cloud Computing Software » Message: [openstack-announce] [OSSA 2014-022] Keystone V2 trusts privilege escalation through user supplied project id (CVE-2014-3520)	Patch Vendor Advisory lists.openstack.org text/html	MLIST [openstack-announce] 20140702 [OSSA 2014-022] Keystone V2 trusts privilege escalation through user supplied project id (CVE-2014-3520)
Security Advisory SA59426 - OpenStack Keystone V2 API Trust Tokens Handling Security Bypass Security Issue - Secunia	Third Party Advisory web.archive.org text/html	SECUNIA 59426
Bug #1331912 "[OSSA 2014-022] V2 Trusts allow trustee to	Exploit	CONFIRM

emulate...” : Bugs : OpenStack Identity (keystone)	Issue Tracking Third Party Advisory bugs.launchpad.net text/html	bugs.launchpad.net/keystone/+bug/1331912
1112668 – (CVE-2014-3520) CVE-2014-3520 openstack-keystone: Keystone V2 trusts privilege escalation through user supplied project id	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1112668

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:openstack:keystone:*:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→