



CVE-2014-3520

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

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

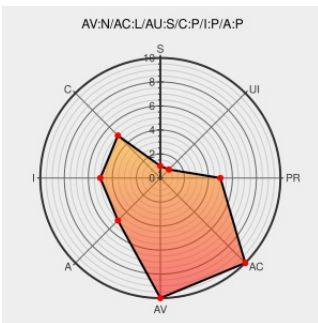
CVE-2014-3520

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

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[access.redhat.com | CVE-2014-3520](https://access.redhat.com/security/cve/CVE-2014-3520)

[access.redhat.com](https://access.redhat.com/security/cve/CVE-2014-3520)
[text/html](https://access.redhat.com/security/cve/CVE-2014-3520)

MISC
access.redhat.com/security/cve/CVE-2014-3520

Red Hat Customer Portal

[access.redhat.com](https://access.redhat.com/errata/RHSA-2014:0994)
[text/html](https://access.redhat.com/errata/RHSA-2014:0994)

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](https://lists.openstack.org/pipermail/openstack-announce/20140702/OSSA_2014-022_Keystone_V2_trusts_privilege_escalation_through_user_supplied_project_id_(CVE-2014-3520).html)
[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](https://web.archive.org/web/20140702000000/http://www.secunia.com/advisories/SA59426.html)
[text/html](#)

SECUNIA 59426

Bug #1331912 "[OSSA 2014-022] V2 Trusts allow trustee to

[Exploit](#)

CONFIRM

bugs.launchpad.net/keystone/+bug/1331912

 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
<code>cpe:2.3:a:openstack:keystone:*.*:~::~:~::~:</code>						
<code>cpe:2.3:a:openstack:keystone:*.*:~::~:~::~:</code>						

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