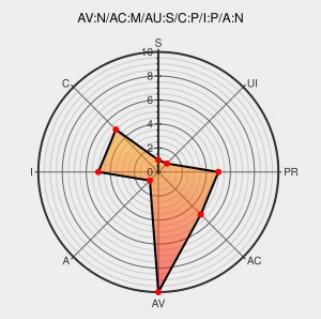
CVE-2014-5252

Published on: 08/25/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:52 PM UTC

CVE-2014-5252

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The V3 API in OpenStack Identity (Keystone) 2014.1.x before 2014.1.2.1 and Juno before Juno-3 updates the issued_at value for UUID v2 tokens, which allows remote authenticated users to bypass the token expiration and retain access via a verification (1) GET or (2) HEAD request to v3/auth/tokens/.

CVE-2014-5252 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
USN-2324-1: OpenStack Keystone vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2324-1
oss-security - [OSSA 2014-026] Multiple vulnerabilities in Keystone revocation events (CVE-2014-5251, CVE-2014-5252, CVE-2014-5253)	www.openwall.com text/html	MLIST [oss-security] 20140815 [OSSA 2014-026] Multiple vulnerabilities in Keystone revocation events (CVE-2014-5251, CVE-2014-5252, CVE-2014-5253)
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2014:1121
Bug #1348820 “[OSSA 2014-026] Token issued_at time changes on /v...” : Bugs : OpenStack Identity (keystone)	bugs.launchpad.net text/html	MISC bugs.launchpad.net/keystone/+bug/1348820

Red Hat Customer Portal web.archive.org text/html Inactive Link Not Archived REDHAT RHSA-2014:1122

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
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Application	Openstack	Keystone	2014.1	All	All	All
Application	Openstack	Keystone	2014.1.2	All	All	All
Application	Openstack	Keystone	juno-1	All	All	All
Application	Openstack	Keystone	juno-2	All	All	All
Application	Openstack	Keystone	2014.1	All	All	All
Application	Openstack	Keystone	2014.1.2	All	All	All
Application	Openstack	Keystone	juno-1	All	All	All
Application	Openstack	Keystone	juno-2	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:a:openstack:keystone:2014.1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:2014.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:juno-1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:juno-2:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:2014.1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:2014.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:juno-1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:juno-2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report