RHSA-2013:0708 - Security Advisory

Issued: 2013-04-04 Updated: 2013-04-04

Synopsis

Moderate: openstack-keystone security and bug fix update

Type/Severity

Security Advisory: Moderate

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

Updated openstack-keystone packages that fix two security issues and various bugs are now available for Red Hat OpenStack Folsom.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability

from the CVE links in the References section.

Description

The openstack-keystone packages provide Keystone, a Python implementation of the OpenStack identity service API, which provides Identity, Token, Catalog, and Policy services.

It was found that Keystone did not correctly handle revoked PKI tokens, allowing users with revoked tokens to retain access to resources they should no longer be able to access. (CVE-2013-1865)

A flaw was found in the way Keystone handled tenant names in token requests. A request containing an excessively long tenant name could cause Keystone to consume a large amount of CPU and memory. With this update, the maximum HTTP request size is limited to 112k. This can be changed via the "max_request_body_size" option in "/etc/keystone/keystone.conf". (CVE-2013-0270)

Red Hat would like to thank the OpenStack project for reporting the CVE-2013-1865 issue. Upstream acknowledges Guang Yee (HP) as the original reporter of CVE-2013-1865. The CVE-2013-0270 issue was discovered by Dan Prince of Red Hat.

This update also fixes various bugs in the openstack-keystone packages.

All users of openstack-keystone are advised to upgrade to these updated packages, which correct these issues. After installing the updated packages, the Keystone service (openstack-keystone) will be restarted automatically.

Solution

Before applying this update, make sure all previously-released errata relevant to your system have been applied.

This update is available via the Red Hat Network. Details on how to use the Red Hat Network to apply this update are available at https://access.redhat.com/knowledge/articles/11258

Affected Products

- Red Hat OpenStack folsom x86_64

Fixes

- BZ - 887815 - a comprehensive keystone.conf file should be included in the RPMS(s)
- BZ - 888575 - Keystone's v2.0 API (the only API) is reported as in beta status
- BZ - 909012 - CVE-2013-0270 OpenStack Keystone: Large HTTP request DoS
- BZ - 917208 - PKI tokens are broken after 24 hours
- BZ - 918159 - PKI tokens too long for memcached keys
- BZ - 922230 - CVE-2013-1865 OpenStack keystone: online validation of Keystone PKI tokens bypasses revocation check

CVEs

- CVE-2013-1865
- CVE-2013-0270

References

- https://access.redhat.com/security/updates/classification/#moderate

---

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.