RHSA-2012:1557 - Security Advisory

Issued: 2012-12-10 Updated: 2012-12-10

Synopsis

Moderate: openstack-keystone security, bug fix, and enhancement 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, multiple bugs, and add enhancements 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.

The openstack-keystone packages have been upgraded to upstream version 2012.2.1, which provides a number of bug fixes and enhancements over the previous version. (BZ#883829)

This update also fixes the following security issues:

A flaw in Keystone allowed an attacker with access to the web and network interfaces to continue using chained tokens linked to tokens that had expired. This would allow the attacker to continue using the tokens despite the parent token being expired, giving them continued access to OpenStack services. (CVE-2012-5563)

It was found that Keystone did not correctly handle users being removed from tenants when Amazon Elastic Compute Cloud (Amazon EC2) style credentials (credentials that are issued in the same format as standard Amazon EC2 credentials) were in use. When a user was removed from a tenant, they retained the privileges provided by that tenant, allowing them to access resources they should no longer have access to. (CVE-2012-5571)

Red Hat would like to thank the OpenStack project for reporting these issues. Upstream acknowledges Anndy as the original reporter of CVE-2012-5563, and Vijaya Erukala as the original reporter of CVE-2012-5571.

All users of openstack-keystone are advised to upgrade to these updated packages, which correct these issues and add these enhancements. 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 - 879402 - CVE-2012-5563 OpenStack: Keystone extension of token validity through token chaining
- BZ - 880399 - CVE-2012-5571 OpenStack: Keystone EC2-style credentials invalidation issue
- BZ - 883829 - Keystone - Update to the latest Folsom stable release 2012.2.1

CVEs

- CVE-2012-5571
- CVE-2012-5563

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/.