Red Hat F

RHSA

12-12-10

Overview

Updated P

Synop

Moderat

Type/

Security

Red H

Identi

View a

Topic

Updatec

bugs, and add enhancements are now available for Red Hat OpenStack Essex.

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 2012.1.3, which provides a number of bug fixes and enhancements over the previous version. (BZ#867029)

This update also fixes the following security issues:

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)

When access to Amazon Elastic Compute Cloud (Amazon EC2) was configured, a file permissions flaw in Keystone allowed a local attacker to view the administrative access and secret values used for authenticating requests to Amazon EC2 services. An attacker could use this flaw to access Amazon EC2 and enable, disable, and modify services and settings. (CVE-2012-5483)

Red Hat would like to thank the OpenStack project for reporting CVE-2012-5571. Upstream acknowledges Vijaya Erukala as the original reporter of CVE-2012-5571. The CVE-2012-5483 issue was discovered by Kurt Seifried of the Red Hat Security Response Team.

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 essex x86_64

Fixes

- BZ - 867029 - Update to the latest Essex stable release 2012.1.3
- BZ - 873447 - CVE-2012-5483 OpenStack: Keystone /etc/keystone/ec2rc secret key exposure
- BZ - 880399 - CVE-2012-5571 OpenStack: Keystone EC2-style credentials invalidation issue

CVEs

- CVE-2012-5483
- CVE-2012-5571

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/.