RHSA-2013:0595 - Security Advisory

Issued: 2013-03-05 Updated: 2013-03-05

Synopsis

Moderate: openstack-packstack 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

An updated openstack-packstack package that fixes two security issues and several bugs is 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

PackStack is a command line utility that uses Puppet modules to support rapid deployment of OpenStack on existing servers over an SSH connection. PackStack is suitable for deploying both single node proof of concept installations and more complex multi-node installations.

A flaw was found in PackStack. During manifest creation, the manifest file was written to /tmp/ with a predictable file name. A local attacker could use this flaw to perform a symbolic link attack, overwriting an arbitrary file accessible to the user running PackStack with the contents of the manifest, which could lead to a denial of service. Additionally, the attacker could read and potentially modify the manifest being generated, allowing them to modify systems being deployed using OpenStack. (CVE-2013-0261)

It was discovered that the cinder.conf and all api-paste.ini configuration files were created with world-readable permissions. A local attacker could use this flaw to view administrative passwords, allowing them to control systems deployed and managed by OpenStack. (CVE-2013-0266)

The CVE-2013-0261 issue was discovered by Kurt Seifried of the Red Hat Security Response Team, and CVE-2013-0266 was discovered by Derek Higgins of the Red Hat OpenStack team.

This update also fixes several bugs in the openstack-packstack package.

All users of openstack-packstack are advised to upgrade to this updated package, which corrects these issues.

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 - 886592 - Openstack Installer: packstack should return an informative error when remote nodes are not configured with openstack repository
- BZ - 890295 - Packstack should not fail installation of cinder-vol service if the VG doesn't exist (as cinder-vol may be using plugins)
- BZ - 892942 - openstack-packstack: When SELinux disabled on machine installation failed with Error during remote puppet apply of horizon.pp.
- BZ - 903187 - Better error handling for missing parameters in answer file
- BZ - 904669 - PackStack should create a simple cinder block storage device to use by default if none is present
- BZ - 905516 - openstack-packstack: Race condition caused /etc/sysconfig/modules/kvm.modules could not be found.
- BZ - 905737 - When using packstack where hostname is localhost.localdomain, mysql fails to install
- BZ - 906006 - The --gen-answer-file parameter does not understand the ~ shortcut for home.
- BZ - 906410 - Generate answer file when running on live mode
- BZ - 907624 - Misleading message when generating public key.
- BZ - 907737 - Typo: Creating Galnce Manifest...
- BZ - 908101 - CVE-2013-0261 OpenStack packstack: insecure use of /tmp in manifest creation
- BZ - 908581 - CVE-2013-0266 OpenStack packstack: puppetlabs-cinder / manifests / base.pp weak file permissions
- BZ - 910211 - Epel version is hardcoded to epel-release-6-8
- BZ - 910818 - packstack should install openstack-selinux
- BZ - 911653 - KeyError in remove_remote_var_dirs

CVEs

- CVE-2013-0266
- CVE-2013-0261

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/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Loading

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit