RHSA-2012:0101 - Security Advisory

Issued: 2012-02-06 Updated: 2012-02-06

Overview

Updated Packages

Synopsis

Low: Red Hat Network Satellite spacewalk-backend security and bug fix update

Type/Severity

Security Advisory: Low

Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

View affected systems

Topic

Updated spacewalk-backend packages that fix one security issue and two bugs are now available for Red Hat Network Satellite 5.4.

The Red Hat Security Response Team has rated this update as having low security impact. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available from the CVE link in the References section.

Description

Red Hat Network (RHN) Satellite is a systems management tool for Linux-based infrastructures. It allows for provisioning, monitoring, and remote management of multiple Linux deployments with a single, centralized tool.

If a user submitted a system registration XML-RPC call to an RHN Satellite server (for example, by running "rhnreg_ks") and that call failed, their RHN user password was included in plain text in the error messages both stored in the server log and mailed to the server administrator. With this update, user passwords are excluded from these error messages to avoid the exposure of authentication credentials. (CVE-2012-0059)

This update also fixes the following bugs:

- When activating a new RHN Satellite certificate that has less

entitlements than is currently used or allotted on the Satellite server, the error message notified the user only about the first problem encountered and did not include directions for resolution. With this update, more verbose error messages are shown in this scenario. (BZ#209514, BZ#704623)

All users of Red Hat Network Satellite are advised to upgrade to these updated packages, which correct these issues. For this update to take effect, Red Hat Network Satellite must be restarted. Refer to the Solution section for details.

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/kb/docs/DOC-11259

Run the following command to restart the Red Hat Network Satellite server:

rhn-satellite restart

Affected Products

- Red Hat Satellite with Embedded Oracle 5.4 for RHEL 6 x86_64
- Red Hat Satellite with Embedded Oracle 5.4 for RHEL 5 x86_64
- Red Hat Satellite with Embedded Oracle 5.4 for RHEL 5 i386

Fixes

- BZ - 749890 - Mask passwords from xmlrpc tracebacks
- BZ - 782819 - CVE-2012-0059 Satellite, Spacewalk: RHN user password disclosure upon failed system registration

CVEs

- CVE-2012-0059

References

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

---

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

All systems operational