Bug 850953 (CVE-2012-5562) - VUL-1: CVE-2012-5562: spacewalk: rhn-proxy: may transmit credentials over clear-text

Status: RESOLVED FIXED

Alias: CVE-2012-5562

Product: SUSE Security Incidents
Component: Incidents (show other bugs)
Version: unspecified
Hardware: Other Other

Priority: P4 - Low **Severity**: Normal
Target Milestone: ---
Deadline: 2014-01-31
Assignee: Security Team bot
QA Contact: Security Team bot

URL:
Whiteboard: .
Keywords:

Depends on:
Blocks:

- Clone This Bug

Reported: 2013-11-18 17:53 UTC by Thomas Biege
Modified: 2014-03-12 12:56 UTC (History)
CC List: 2 users (show)

See Also:
Found By: ---
Services Priority:
Business Priority:
Blocker: ---

Attachments

Add an attachment (proposed patch, testcase, etc.)

Note

You need to log in before you can comment on or make changes to this bug.

Marcus Meissner 2014-03-12 12:56:17 UTC Comment 10

```
was only released in satellite 5.6

https://access.redhat.com/security/cve/CVE-2012-5562
https://bugzilla.redhat.com/show_bug.cgi?id=879369

It was found that when RHN Proxy was used as a proxy to connect to RHN Satellite,
certain pages that should have been protected via SSL (in direct to Satellite
connections) were in fact only protected between RHN Proxy and RHN Satellite; the
connection between the client and RHN Proxy was not protected via SSL.  This could
leak confidential information or authentication credentials when accessing RHN
Satellite via RHN Proxy.
```

```
By default, yum clients and rhn_register will always communicate with RHN Proxy
over HTTPS.
```

Format For Printing - XML - Clone This Bug - Top of page