

Bug 850953 (CVE-2012-5562) - VUL-1: CVE-2012-5562: spacewalk: rhn-proxy: may transmit credentials over clear-text**Status:** RESOLVED FIXED[Clone This Bug](#)**Alias:** CVE-2012-5562**Reported:** 2013-11-18 17:53 UTC by Thomas Biege**Modified:** 2014-03-12 12:56 UTC ([History](#))**Product:** SUSE Security Incidents**CC List:** 2 users ([show](#))**Component:** Incidents ([show other bugs](#))**Version:** unspecified**See Also:****Hardware:** Other Other**Found By:** ---**Priority:** P4 - Low **Severity:** Normal**Services Priority:****Target Milestone:** ---**Business Priority:****Deadline:** 2014-01-31**Blocker:** ---**Assignee:** Security Team bot**QA Contact:** Security Team bot**URL:****Whiteboard:** .**Keywords:****Depends on:****Blocks:****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](#)