



## Bug 681032 (CVE-2011-2920) - CVE-2011-2920 Satellite: XSS flaw(s) in filter handling

**Keywords:**

**Reported:** 2011-02-28 21:37 UTC by Vincent Danen

**Status:** CLOSED ERRATA

**Modified:** 2023-05-11 17:11 UTC ([History](#))

**Alias:** CVE-2011-2920

**CC List:** 11 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:** 2011-09-15 21:25:12 UTC

**Hardware:** All

**Embargoed:**

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Red Hat Product Security

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** 730927

**Blocks:** 622406 713496

**TreeView+** [depends on](#) / [blocked](#)

### Attachments [\(Terms of Use\)](#)

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2011:1299</a>	0	normal	SHIPPED_LIVE	Moderate: Red Hat Network Satellite server security and enhancement update	2011-09-15 17:54:55 UTC

Vincent Danen 2011-02-28 21:37:54 UTC

[Description](#)

Nils Juenemann reported that there is a cross-site scripting flaw in the filter for a result set in nearly every filter

form provided by Red Hat Satellite (for example the "Filter by Synopsis" field).

Acknowledgements:

Red Hat would like to thank Nils Juenemann and The Bearded Warriors for independently reporting this issue.

Vincent Danen 2011-05-09 16:42:43 UTC

[Comment 3](#)

This also affects upstream Spacewalk 1.4, as reported by The Bearded Warriors.

errata-xmlrpc 2011-09-15 17:55:04 UTC

[Comment 15](#)

This issue has been addressed in following products:

Red Hat Network Satellite Server v 5.4

Via RHSA-2011:1299 <https://rhn.redhat.com/errata/RHSA-2011-1299.html>

Jan Pazdziora (Red Hat) 2011-09-16 09:32:55 UTC

[Comment 16](#)

Fixed in Spacewalk master, commit e91fab3da553f37d58aa43c067347010e8c95225, tagged as spacewalk-java-1.6.46-1.

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

