



# Spacewalk: spacewalk: cross-site scripting vulnerability allows arbitrary web script execution.

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2011-2920  |
| <b>State</b>           | PUBLISHED  |
| <b>Assigner</b>        | redhat   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2014-02-05 18:55:05 UTC  |
| <b>Updated</b>         | 2026-04-02 22:16:23 UTC  |
| <b>Description</b>     | A flaw was found in Spacewalk and Red Hat Network Satellite. This cross-site scripting (XSS) vulnerability allows a remote |

## Risk And Classification

**Primary CVSS:** v3.1 5.5 MEDIUM from secalert@redhat.com

**CVSS:**3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L

**EPSS:** 0.003220000 probability, percentile 0.552270000 (date 2026-04-02)

**Problem Types:** CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

| Version | Source              | Type    | Score | Severity | Vector                                       |
|---------|---------------------|---------|-------|----------|--|
| 3.1     | secalert@redhat.com | Primary | 5.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L |
| 3.1     | CNA                 | CVSS    | 5.5   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L |
| 2.0     | nvd@nist.gov        | Primary | 4.3   |          | AV:N/AC:M/Au:N/C:N/I:P/A:N                   |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

Low

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

### NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product           | Version | Update | Edition | Language |
|-------------|--------|-------------------|---------|--------|---------|----------|
| Application | Redhat | Network Satellite | -       | All    | All     | All      |
| Application | Redhat | Spacewalk         | 1.6     | All    | All     | All      |

### Vendor Declared Affected Products

| Source | Vendor  | Product                    | Version       | Platforms     |
|--------|---------|----------------------------|---------------|---------------|
| CNA    | Red Hat | Red Hat Enterprise Linux 6 | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 6 | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 6 | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 7 | Not specified | Not specified |
| CNA    | Red Hat | Red Hat Enterprise Linux 7 | Not specified | Not specified |

### References

| Reference                               | Source              | Link       |
|---|---------------------|------------|
| CVE-2011-2920 - Red Hat Customer Portal | secalert@redhat.com | access.red |

|  |                                      |   |
|--|--------------------------------------|---|
| Support  | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.redhat.com">www.redhat.com</a>            |
| [Spacewalk-announce-list] Spacewalk 1.6 has been released                        | af854a3a-2127-422b-91ae-364da2661108 | <a href="http://www.redhat.com">www.redhat.com</a>            |
| 681032 – (CVE-2011-2920) CVE-2011-2920 Satellite: XSS flaw(s) in filter handling | af854a3a-2127-422b-91ae-364da2661108 | <a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a> |
| Red Hat Customer Portal  | MITRE                                | <a href="https://access.redhat.com">access.redhat.com</a>     |
| CVE Program record   | CVE.ORG                              | <a href="http://www.cve.org">www.cve.org</a>                  |
| NVD vulnerability detail   | NVD                                  | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                |

No vendor comments have been submitted for this CVE.

#### Additional Advisory Data

| Source | Time                     | Event                |
|--------|--------------------------|----------------------|
| CNA    | 2026-04-02T15:01:09.526Z | Reported to Red Hat. |
| CNA    | 2014-02-05T18:00:00.000Z | Made public.         |

#### Workarounds

**CNA:** Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)