



About cookies on this site

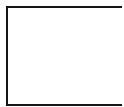


CVE

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

VEX [↗](#)
Public
Last mo

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.



In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for

Accept Default

Do Not Sell or Share My Personal Information

Description	Mitigation	Additional information	Affected Packages	CVSS Score Details	Weakness (CWE)	FAQ
-------------	------------	------------------------	-------------------	--------------------	----------------	-----

Description

A flaw was found in Spacewalk and Red Hat Network Satellite. This vulnerability, known as cross-site scripting (XSS), allows remote attackers to inject malicious web scripts or HTML into web pages viewed by other users. The flaw is triggered through vectors related to Search forms, enabling attackers to potentially steal sensitive information or perform actions on behalf of the victim.

Mitigation

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.

Additional information

- [CWE-79: Improper Neutralization of Input During Web Page Generation \('Cross-site Scripting'\)](#)
- [FAQ: Frequently asked questions about CVE-2011-2927](#)

External references

- <https://www.cve.org/CVERecord?id=CVE-2011-2927>
- <https://nvd.nist.gov/vuln/detail/CVE-2011-2927>
- <http://www.redhat.com/support/errata/RHSA-2011-1299.html>
- https://bugzilla.redhat.com/show_bug.cgi?id=730955
- <https://www.redhat.com/archives/spacewalk-announce-list/2011-December/msg00000.html>

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by:

Products / Services

Components

State

Errata

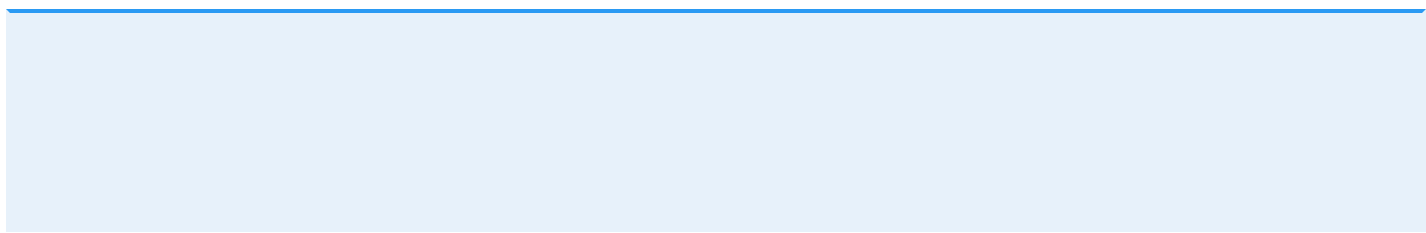
[Clear all](#)

Products / Services	Red Hat Enterprise Linux 6
Components	rhn-client-tools
State	Out of support scope
Justification	None
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 6
Components	rhnsd
State	Out of support scope
Justification	None
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 6
Components	yum-rhn-plugin
State	Out of support scope
Justification	None
Errata	

Common Vulnerability Scoring System (CVSS) Score Details



Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	5.4	N/A	N/A
Attack Vector	Network	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	None	N/A	N/A
User Interaction	Required	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	Low	N/A	N/A
Integrity Impact	Low	N/A	N/A
Availability Impact	None	N/A	N/A

CVSS v3 Vector

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

Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors?	▼
My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?	▼
What can I do if my product is listed as "Will not fix"?	▼
What can I do if my product is listed as "Fix deferred"?	▼
What is a mitigation?	▼
I have a Red Hat product but it is not in the above list, is it affected?	▼
Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?	▼
My product is listed as "Out of Support Scope". What does this mean?	▼

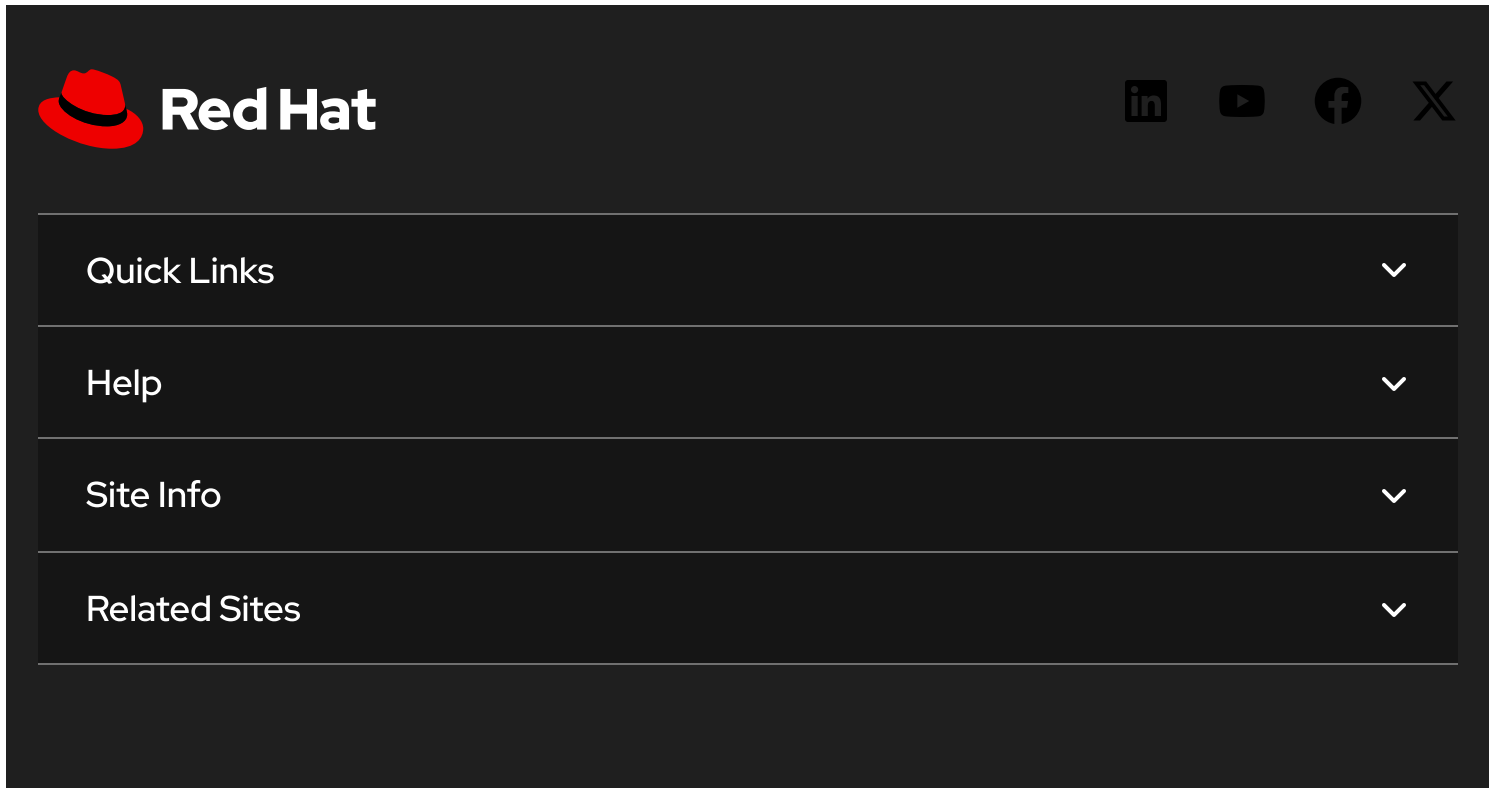
Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.


For clarification or corrections, please contact [Red Hat Product Security](#).

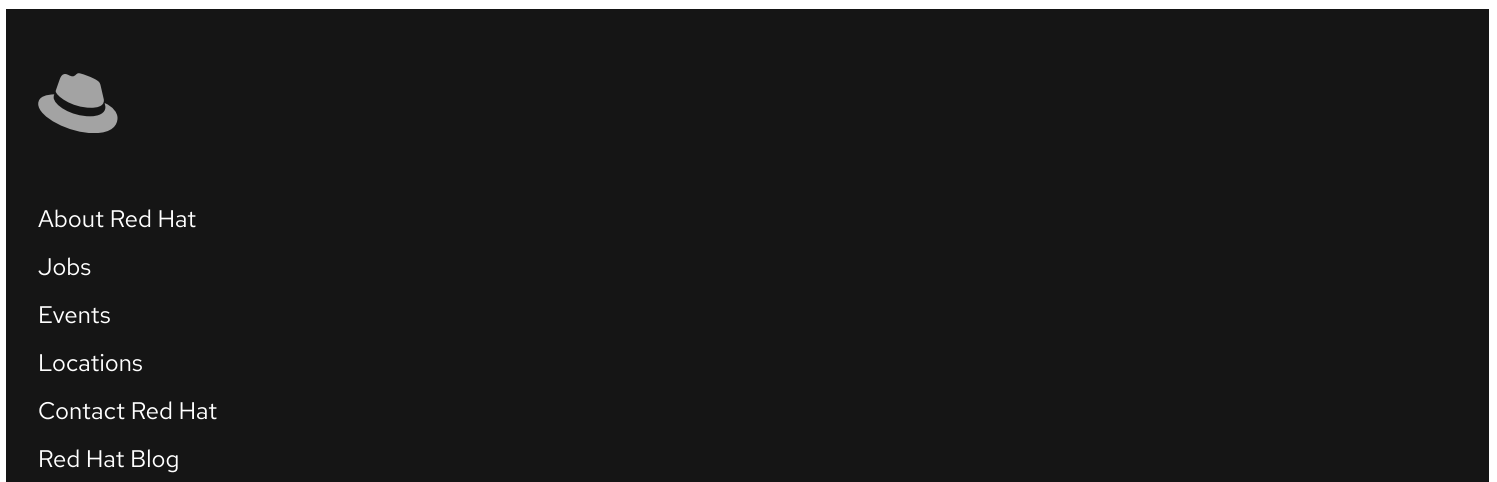
Last modified: April 2, 2026 at 11:42:20 PM UTC

CVE description copyright © 2021



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, consisting of a red fedora hat icon and the text "Red Hat" in white. On the right are four social media icons: LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of four menu items, each with a white downward-pointing chevron icon on the right: "Quick Links", "Help", "Site Info", and "Related Sites".

 Partial system outage



The image shows a dark-themed footer menu. It starts with a small, light-colored fedora hat icon. Below the icon is a vertical list of six links: "About Red Hat", "Jobs", "Events", "Locations", "Contact Red Hat", and "Red Hat Blog".

[Inclusion at Red Hat](#)

[Cool Stuff Store](#)

[Red Hat Summit](#)

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Do Not Sell or Share My Personal Information](#)