



Red Hat Product Errata    RHSA-2026:0076 - Security Advisory

# RHSA-2026:0076 - Security Advisory

Issued: 2026-01-05    Updated: 2026-01-05

[Overview](#)

[Updated Packages](#)

## Synopsis

Important: spice-client-win security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for spice-client-win is now available for Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support, Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions, and Red Hat Enterprise Linux 8.6 Telecommunications Update Service.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

## Description

Spice client MSI installers for Windows clients

Security Fix(es):

- sqlite: Integer Truncation in SQLite (CVE-2025-6965)
- libtiff: LibTIFF Use-After-Free Vulnerability (CVE-2025-8176)
- libtiff: Libtiff Write-What-Where (CVE-2025-9900)
- expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing (CVE-2025-59375)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

## Solution





For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 


## Affected Products

- Red Hat Enterprise Linux for x86\_64 - Extended Update Support Extension 8.6 x86\_64
- Red Hat Enterprise Linux Server - AUS 8.6 x86\_64
- Red Hat Enterprise Linux Server - TUS 8.6 x86\_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 8.6 x86\_64

## Fixes

- BZ - 2380149  - CVE-2025-6965 sqlite: Integer Truncation in SQLite
- BZ - 2383598  - CVE-2025-8176 libtiff: LibTIFF Use-After-Free Vulnerability
- BZ - 2392784  - CVE-2025-9900 libtiff: Libtiff Write-What-Where
- BZ - 2395108  - CVE-2025-59375 expat: libexpat in Expat allows attackers to trigger large dynamic memory allocations via a small document that is submitted for parsing

## CVEs

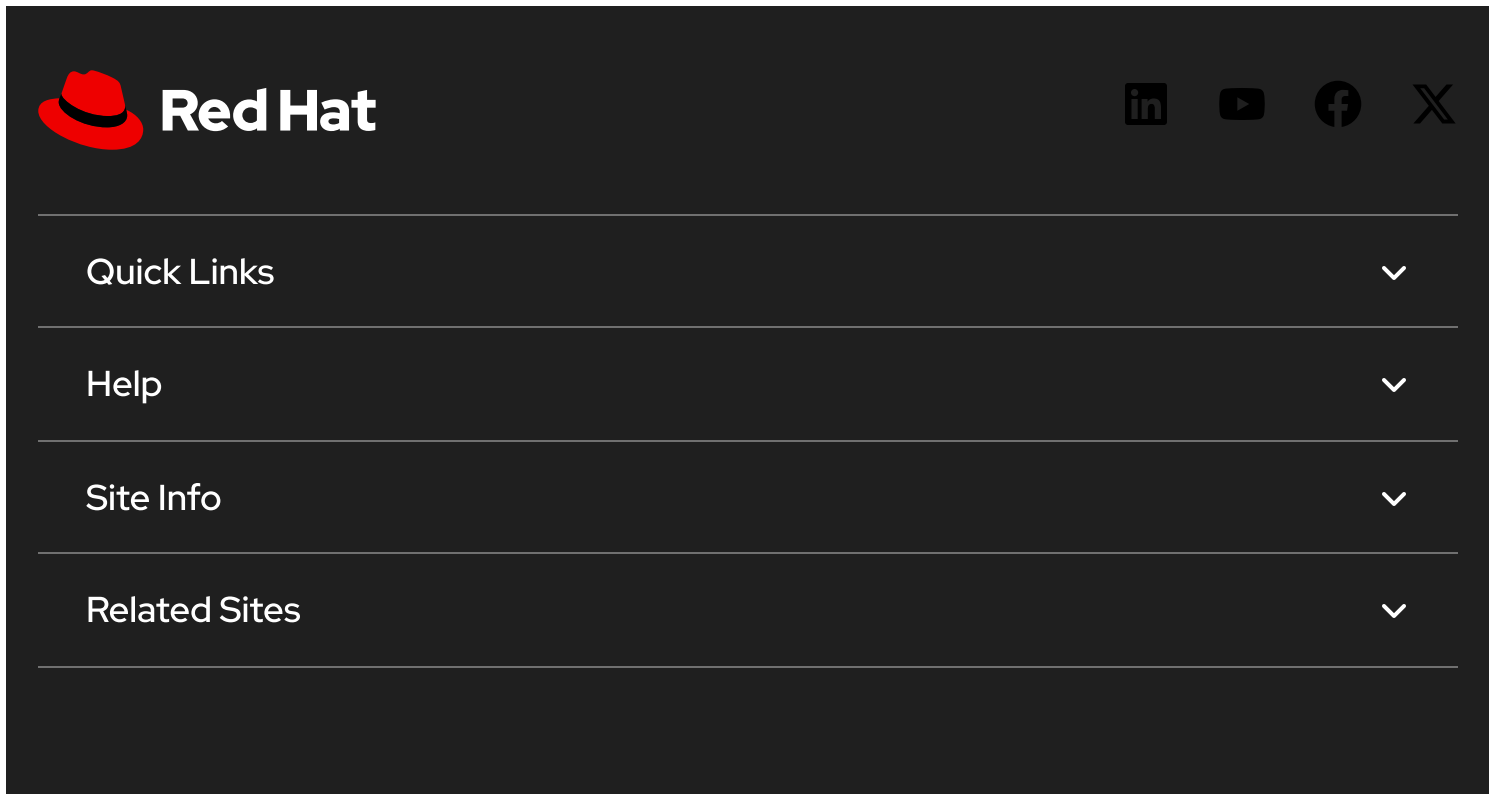
- CVE-2025-6965 

- [CVE-2025-8176](#) ↗
- [CVE-2025-9900](#) ↗
- [CVE-2025-59375](#) ↗

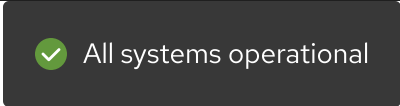
## References

- <https://access.redhat.com/security/updates/classification/#important> ↗

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



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". On the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of menu items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right, indicating a dropdown menu.



A dark grey notification box with a green checkmark icon on the left and the text "All systems operational" in white.



The footer area features a dark background with a small grey fedora hat icon on the left. To the right of the icon is a vertical list of navigation links: "About Red Hat", "Jobs", "Events", "Locations", and "Contact Red Hat".

[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 Opt-Out Rights](#)