RHSA-2026:1570 - Security Advisory

Issued: 2026-01-29 Updated: 2026-01-29

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):

- libsoup: libsoup: Duplicate Host Header Handling Causes Host-Parsing Discrepancy (First- vs Last-Value Wins) (CVE-2025-14523)

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 - 2421349 - CVE-2025-14523 libsoup: libsoup: Duplicate Host Header Handling Causes Host-Parsing Discrepancy (First- vs Last-Value Wins)

CVEs

- CVE-2025-14523

References

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

---

The Red Hat security contact is secalert@redhat.com. More contact details at https://access.redhat.com/security/team/contact/.

Red Hat

Quick Links

Help

Site Info

Related Sites

All systems operational

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility