



Red Hat Product Errata RHSA-2026:2182 - Security Advisory

RHSA-2026:2182 - Security Advisory

Issued: 2026-02-05 Updated: 2026-02-05

[Overview](#)

[Updated Packages](#)

Synopsis

Important: libsoup3 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 libsoup3 is now available for Red Hat Enterprise Linux 10.

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

Libsoup is an HTTP library implementation in C. It was originally part of a SOAP (Simple Object Access Protocol) implementation called Soup, but the SOAP and non-SOAP parts have now been split into separate packages. libsoup uses the Glib main loop and is designed to work well with GTK applications. This enables GNOME applications to access HTTP servers on the network in a completely asynchronous fashion, very similar to the Gtk+ programming model (a synchronous operation mode is also supported for those who want it), but the SOAP parts were removed long ago.

Security Fix(es):

- libsoup: Signed to Unsigned Conversion Error Leading to Stack-Based Buffer Overflow in libsoup NTLM Authentication (CVE-2026-0719)
- libsoup: Stack-Based Buffer Overflow in libsoup Multipart Response Parsingmultipart HTTP response (CVE-2026-1761)

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 10 x86_64
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- Red Hat CodeReady Linux Builder for x86_64 10 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 10 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x

Fixes

- BZ - 2427906  - CVE-2026-0719 libsoup: Signed to Unsigned Conversion Error Leading to Stack-Based Buffer Overflow in libsoup NTLM Authentication
- BZ - 2435961  - CVE-2026-1761 libsoup: Stack-Based Buffer Overflow in libsoup Multipart Response Parsingmultipart HTTP response

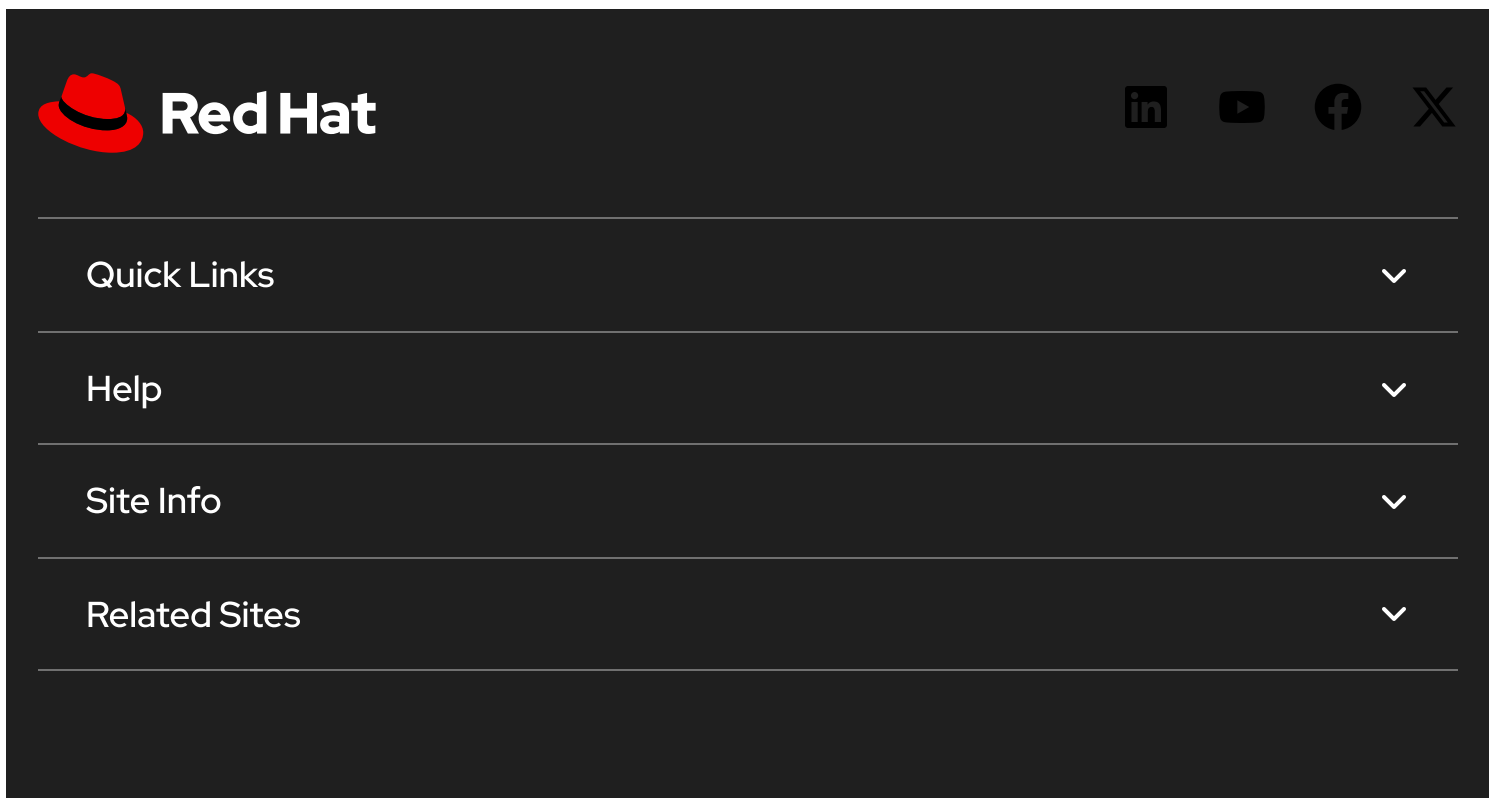
CVEs

- [CVE-2026-0719](#) ↗
- [CVE-2026-1761](#) ↗

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/>.



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: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right, indicating a dropdown menu.

✓ All systems operational



The image shows a dark-themed footer navigation menu. On the left is a small, light-colored fedora hat icon. To its right are three text links: "About Red Hat", "Jobs", and "Events", all in a light gray color.

[Locations](#)

[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](#)