



Red Hat F

# RHSA Advis



i-02-05

Overview

Updated P

## Synop

Importa

## 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 libsoup is now available for Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions.

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

The libsoup packages provide an HTTP client and server library for GNOME.

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 Server - AUS 9.2 x86\_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.2 x86\_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 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](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



---

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](#)

---

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Opt-Out Rights](#)