



Red Hat Product Errata    RHSA-2025:8140 - Security Advisory

# RHSA-2025:8140 - Security Advisory

Issued: 2025-05-26    Updated: 2025-05-26

[Overview](#)[Updated Packages](#)

## Synopsis

Important: libsoup 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 libsoup is now available for Red Hat Enterprise Linux 9.2 Extended Update Support.

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: Heap buffer over-read in `skip\_insignificant\_space` when sniffing content (CVE-2025-2784)
- libsoup: Denial of Service attack to websocket server (CVE-2025-32049)
- libsoup: OOB Read on libsoup through function "soup\_multipart\_new\_from\_message" in soup-multipart.c leads to crash or exit of process (CVE-2025-32914)
- libsoup: Integer Underflow in soup\_multipart\_new\_from\_message() Leading to Denial of Service in libsoup (CVE-2025-4948)

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 9.2 x86\_64
- Red Hat Enterprise Linux Server - AUS 9.2 x86\_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64
- 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
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 9.2 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x

## Fixes

- [BZ - 2354669](#) - CVE-2025-2784 libsoup: Heap buffer over-read in `skip\_insignificant\_space` when sniffing content
- [BZ - 2357066](#) - CVE-2025-32049 libsoup: Denial of Service attack to websocket server
- [BZ - 2359358](#) - CVE-2025-32914 libsoup: OOB Read on libsoup through function "soup\_multipart\_new\_from\_message" in soup-multipart.c leads to crash or exit of process
- [BZ - 2367183](#) - CVE-2025-4948 libsoup: Integer Underflow in soup\_multipart\_new\_from\_message() Leading to Denial of Service in libsoup

## CVEs

- [CVE-2025-2784](#)
- [CVE-2025-4948](#)
- [CVE-2025-32049](#)
- [CVE-2025-32914](#)

## 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](#)