RHSA-2025:8481 - Security Advisory

Issued: 2025-06-04 Updated: 2025-06-04

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 9.0 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: 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 Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 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. More contact details at https://access.redhat.com/security/team/contact/.