RHSA-2025:21657 - Security Advisory

Issued: 2025-11-18 Updated: 2025-11-18

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 7 Extended Lifecycle 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: Out of bounds reads in soup_headers_parse_request() (CVE-2025-32906)
- libsoup: Double free on soup_message_headers_get_content_disposition() through "soup-message-headers.c" via "params" GHashTable value (CVE-2025-32911)
- libsoup: NULL pointer dereference in soup_message_headers_get_content_disposition when "filename" parameter is present, but has no value in Content-Disposition header (CVE-2025-32913)
- 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 Overflow in Cookie Expiration Date Handling in libsoup (CVE-2025-4945)
- libsoup: Integer Underflow in soup_multipart_new_from_message() Leading to Denial of Service in libsoup (CVE-2025-4948)
- libsoup: Out-of-Bounds Read in Cookie Date Handling of libsoup HTTP Library (CVE-2025-11021)

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 - Extended Life Cycle Support 7 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le

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 - 2359341 - CVE-2025-32906 libsoup: Out of bounds reads in soup_headers_parse_request()
- BZ - 2359355 - CVE-2025-32911 libsoup: Double free on soup_message_headers_get_content_disposition() through "soup-message-headers.c" via "params" GHashTable value
- BZ - 2359357 - CVE-2025-32913 libsoup: NULL pointer dereference in soup_message_headers_get_content_disposition when "filename" parameter is present, but has no value in Content-Disposition header
- 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 - 2367175 - CVE-2025-4945 libsoup: Integer Overflow in Cookie Expiration Date Handling in libsoup
- BZ - 2367183 - CVE-2025-4948 libsoup: Integer Underflow in soup_multipart_new_from_message() Leading to Denial of Service in libsoup
- BZ - 2399627 - CVE-2025-11021 libsoup: Out-of-Bounds Read in Cookie Date Handling of libsoup HTTP Library

CVEs

- CVE-2025-2784
- CVE-2025-4945
- CVE-2025-4948
- CVE-2025-11021
- CVE-2025-32049
- CVE-2025-32906
- CVE-2025-32911
- CVE-2025-32913
- 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/.

Quick Links

Help

Site Info

Related Sites

⚠ Service under maintenance

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
Cookie Preferences and Opt-Out Rights