RHSA-2025:4440 - Security Advisory

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

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 9.4 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: Integer overflow in append_param_quoted (CVE-2025-32050)
- libsoup: Heap buffer overflow in sniff_unknown() (CVE-2025-32052)
- libsoup: Heap buffer overflows in sniff_feed_or_html() and skip_insignificant_space() (CVE-2025-32053)
- libsoup: Out of bounds reads in soup_headers_parse_request() (CVE-2025-32906)
- libsoup: Denial of service in server when client requests a large amount of overlapping ranges with Range header (CVE-2025-32907)
- 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: Information disclosure may leads libsoup client sends Authorization header to a different host when being redirected by a server (CVE-2025-46421)
- libsoup: Memory leak on soup_header_parse_quality_list() via soup-headers.c (CVE-2025-46420)

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 9.4 x86_64
- Red Hat Enterprise Linux Server - AUS 9.4 x86_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
- Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64

- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x
- Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x

Fixes

- BZ - 2357067 - CVE-2025-32050 libsoup: Integer overflow in append_param_quoted
- BZ - 2357069 - CVE-2025-32052 libsoup: Heap buffer overflow in sniff_unknown()
- BZ - 2357070 - CVE-2025-32053 libsoup: Heap buffer overflows in sniff_feed_or_html() and skip_insignificant_space()
- BZ - 2359341 - CVE-2025-32906 libsoup: Out of bounds reads in soup_headers_parse_request()
- BZ - 2359342 - CVE-2025-32907 libsoup: Denial of service in server when client requests a large amount of overlapping ranges with Range header
- 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 - 2361962 - CVE-2025-46421 libsoup: Information disclosure may leads libsoup client sends Authorization header to a different host when being redirected by a server
- BZ - 2361963 - CVE-2025-46420 libsoup: Memory leak on soup_header_parse_quality_list() via soup-headers.c

CVEs

- CVE-2025-32050
- CVE-2025-32052
- CVE-2025-32053
- CVE-2025-32906
- CVE-2025-32907
- CVE-2025-32911
- CVE-2025-32913
- CVE-2025-46420
- CVE-2025-46421

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/.