RHSA-2025:7505 - Security Advisory

Issued: 2025-05-13 Updated: 2025-05-13

Synopsis

Important: libsoup3 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 libsoup3 is now available for Red Hat Enterprise Linux 10.

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

Libsoup is an HTTP library implementation in C. It was originally part of a SOAP (Simple Object Access Protocol) implementation called Soup, but the SOAP and non-SOAP parts have now been split into separate packages. libsoup uses the Glib main loop and is designed to work well with GTK applications. This enables GNOME applications to access HTTP servers on the network in a completely asynchronous fashion, very similar to the Gtk+ programming model (a synchronous operation mode is also supported for those who want it), but the SOAP parts were removed long ago.

Security Fix(es):

- libsoup: Heap buffer over-read in `skip_insignificant_space` when sniffing content (CVE-2025-2784)
- libsoup: Out of bounds reads in soup_headers_parse_request() (CVE-2025-32906)
- libsoup: Denial of service on libsoup through HTTP/2 server (CVE-2025-32908)
- libsoup: NULL pointer dereference in client when server omits the "nonce" parameter in an Unauthorized response with Digest authentication (CVE-2025-32912)
- 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: Information disclosure may leads libsoup client sends Authorization header to a different host when being redirected by a server (CVE-2025-46421)

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 10 x86_64
- Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat Enterprise Linux for IBM z Systems 10 s390x
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian 10 ppc64le
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for ARM 64 10 aarch64
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64

- Red Hat CodeReady Linux Builder for x86_64 10 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le
- Red Hat CodeReady Linux Builder for ARM 64 10 aarch64
- Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x
- Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64
- Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le
- Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64

Fixes

- BZ - 2354669 - CVE-2025-2784 libsoup: Heap buffer over-read in `skip_insignificant_space` when sniffing content
- BZ - 2359341 - CVE-2025-32906 libsoup: Out of bounds reads in soup_headers_parse_request()
- BZ - 2359343 - CVE-2025-32908 libsoup: Denial of service on libsoup through HTTP/2 server
- BZ - 2359356 - CVE-2025-32912 libsoup: NULL pointer dereference in client when server omits the "nonce" parameter in an Unauthorized response with Digest authentication
- 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 - 2361962 - CVE-2025-46421 libsoup: Information disclosure may leads libsoup client sends Authorization header to a different host when being redirected by a server
- RHEL-84737 - Rebase to 3.6.5
- RHEL-65395 - server-test failure

CVEs

- CVE-2025-2784
- CVE-2025-32906
- CVE-2025-32908
- CVE-2025-32912
- CVE-2025-32914
- 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/.