



Red Hat Product Errata    RHSA-2025:8292 - Security Advisory

# RHSA-2025:8292 - Security Advisory

Issued: 2025-05-29    Updated: 2025-05-29

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

## Synopsis

Important: mingw-freetype and spice-client-win 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 mingw-freetype and spice-client-win is now available for Red Hat Enterprise Linux 8.

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

MinGW Windows Freetype library.

Security Fix(es):

- freetype: OOB write when attempting to parse font subglyph structures related to TrueType GX and variable font files (CVE-2025-27363)
- 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: NULL Pointer Dereference on libsoup through function "sniff\_mp4" in `soup-content-sniffer.c` (CVE-2025-32909)
- libsoup: Null pointer dereference on libsoup via `/auth/soup-auth-digest.c` through "soup\_auth\_digest\_authenticate" on client when server omits the "realm" parameter in an Unauthorized response with Digest authentication (CVE-2025-32910)
- 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)

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 8 x86\_64
- Red Hat Enterprise Linux for IBM z Systems 8 s390x
- Red Hat Enterprise Linux for Power, little endian 8 ppc64le
- Red Hat Enterprise Linux for ARM 64 8 aarch64
- Red Hat CodeReady Linux Builder for x86\_64 8 x86\_64

- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 8.10 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x

## Fixes

- [BZ - 2351357](#)  - CVE-2025-27363 freetype: OOB write when attempting to parse font subglyph structures related to TrueType GX and variable font files
- [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 - 2359353](#)  - CVE-2025-32909 libsoup: NULL Pointer Dereference on libsoup through function "sniff\_mp4" in soup-content-sniffer.c
- [BZ - 2359354](#)  - CVE-2025-32910 libsoup: Null pointer dereference on libsoup via /auth/soup-auth-digest.c through "soup\_auth\_digest\_authenticate" on client when server omits the "realm" parameter in an Unauthorized response with Digest authentication
- [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

## CVEs

- [CVE-2025-27363](#) 
- [CVE-2025-32050](#) 
- [CVE-2025-32052](#) 
- [CVE-2025-32053](#) 
- [CVE-2025-32906](#) 
- [CVE-2025-32907](#) 
- [CVE-2025-32909](#) 
- [CVE-2025-32910](#) 
- [CVE-2025-32911](#) 
- [CVE-2025-32913](#) 

## 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 

 Partial system outage



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 and Opt-Out Rights](#)