



Red Hat F

# RHSA Advis



25-12-11

Overview

Updated P

## Synop

Importa

## 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 webkit2gtk3 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

WebKitGTK is the port of the portable web rendering engine WebKit to the GTK platform.

Security Fix(es):

- webkit: WebKitGTK / WPE WebKit: Out-of-bounds read and integer underflow vulnerability leading to DoS (CVE-2025-13502)
- webkitgtk: A website may exfiltrate image data cross-origin (CVE-2025-43392)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43425)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43427)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43429)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43430)
- webkitgtk: Processing maliciously crafted web content may lead to memory corruption (CVE-2025-43431)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43432)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected Safari crash (CVE-2025-43434)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43440)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43443)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43421)
- webkit: WebKitGTK: Remote user-assisted information disclosure via file drag-and-drop (CVE-2025-13947)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-43458)
- webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash (CVE-2025-66287)

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 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 - 2416300](#)  - CVE-2025-13502 webkit: WebKitGTK / WPE WebKit: Out-of-bounds read and integer underflow vulnerability leading to DoS
- [BZ - 2416325](#)  - CVE-2025-43392 webkitgtk: A website may exfiltrate image data cross-origin
- [BZ - 2416327](#)  - CVE-2025-43425 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2416329](#)  - CVE-2025-43427 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2416330](#)  - CVE-2025-43429 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2416331](#)  - CVE-2025-43430 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2416332](#)  - CVE-2025-43431 webkitgtk: Processing maliciously crafted web content may lead to memory corruption
- [BZ - 2416334](#)  - CVE-2025-43432 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2416335](#)  - CVE-2025-43434 webkitgtk: Processing maliciously crafted web content may lead to an unexpected Safari crash
- [BZ - 2416336](#)  - CVE-2025-43440 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2416337](#)  - CVE-2025-43443 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash

- [BZ - 2416355](#)  - CVE-2025-43421 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2418576](#)  - CVE-2025-13947 webkit: WebKitGTK: Remote user-assisted information disclosure via file drag-and-drop
- [BZ - 2418855](#)  - CVE-2025-43458 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash
- [BZ - 2418857](#)  - CVE-2025-66287 webkitgtk: Processing maliciously crafted web content may lead to an unexpected process crash

## CVEs

- [CVE-2025-13502](#) 
- [CVE-2025-13947](#) 
- [CVE-2025-43392](#) 
- [CVE-2025-43421](#) 
- [CVE-2025-43425](#) 
- [CVE-2025-43427](#) 
- [CVE-2025-43429](#) 
- [CVE-2025-43430](#) 
- [CVE-2025-43431](#) 
- [CVE-2025-43432](#) 
- [CVE-2025-43433](#) 
- [CVE-2025-43434](#) 
- [CVE-2025-43438](#) 
- [CVE-2025-43440](#) 
- [CVE-2025-43441](#) 
- [CVE-2025-43443](#) 
- [CVE-2025-43458](#) 
- [CVE-2025-66287](#) 

## 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



✔ All systems operational



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