



# Cookie Preferences and Opt-Out Rights Your Choices About Cookies on this Site



Red Hat F

A cookie is a small amount of data that is sent to your browser from a web server and stored on your device. The cookie may be placed by Red Hat or by an authorized third party.

**RHSA**

25-12-18

Overview

When you use this site, Red Hat uses cookies and other technologies which are necessary to enable the basic features of the site to function (Required cookies). Subject to your preferences, Red Hat and its authorized partners may also use cookies to analyze your use of the website to evaluate and improve our performance, to improve our service to you and to personalize your experience (Functional cookies) as well as advertising cookies to show you ads that are more relevant to you (Advertising cookies). We honor the preferences you select.

Updated P

**Synop**

In addition to the services they provide to Red Hat, certain Red Hat authorized partners may also use this data for their own purposes or for targeted advertising. This activity may qualify as a "sale" or "targeted advertising" under certain data protection laws. You can make choices using the buttons below to allow or prevent such uses.

Importa

**Type/**

Security

**Accept default** will keep your preferences set to accept all cookies (Required, Functional and Advertising), which enables us to provide you a personalized web experience and more relevant ads on third party websites. This means that you allow our partners to collect and use this data.

Red H
Identifi
View a

**Required Cookies only** will set your cookie preferences to "Required Cookies" only. This will prevent our partners from collecting and using this data but may also prevent us from providing you a personalized web experience and more relevant ads on third party websites. Cookie preferences will provide further information and allow you to customize your cookie settings. Setting your cookie preferences to "Required Cookies only" will opt you out of "sales" and "targeted advertising".

**Topic**

Clearing your browser cookies may delete your cookie preferences. If you re-visit this site after clearing browser cookies, you will need to reset your preferences at that time. If you have set your browser's global privacy

An upda  
Support.

te

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 - 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 - 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



Loading



[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