



# About cookies on this site

## CVE

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.

VEX [↗](#)

Public

Last mo

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.

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

**Accept Default**

**Do Not Sell or Share My Personal Information**

Description	Additional information	Affected Packages	CVSS Score Details	Weakness (CWE)	Acknowledgements	FAQ
-------------	------------------------	-------------------	--------------------	----------------	------------------	-----

## Description

An API design flaw in WebKitGTK and WPE WebKit allows untrusted web content to unexpectedly perform IP connections, DNS lookups, and HTTP requests. Applications expect to use the WebPage::send-request signal handler to approve or reject all network requests. However, certain types of HTTP requests bypass this signal handler.

## Additional information

- Bugzilla 2424652: webkitgtk: Authorization bypass through WebPage::send-request signal handler
- CWE-639: Authorization Bypass Through User-Controlled Key

## External references

- <https://www.cve.org/CVERecord?id=CVE-2025-66286>
- <https://nvd.nist.gov/vuln/detail/CVE-2025-66286>
- [https://bugs.webkit.org/show\\_bug.cgi?id=259787](https://bugs.webkit.org/show_bug.cgi?id=259787)

## Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by:

Products / Services

Components

State

Errata

[Clear all](#)

---

**Products / Services** Red Hat Enterprise Linux 6

**Components** webkitgtk

**State** Out of support scope

**Justification** None

**Errata**

**Release Date**

---

**Products / Services**

Red Hat Enterprise Linux 7

**Components**

webkitgtk3

**State**

Will not fix

**Justification**

None

**Errata****Release Date****Products / Services**

Red Hat Enterprise Linux 7

**Components**

webkitatk4

<< < 1 of 1 > >>

## Common Vulnerability Scoring System (CVSS) Score Details

### Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

The following CVSS metrics and score provided are preliminary and subject to review.

### CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
<b>CVSS v3 Base Score</b>	4.7	N/A	N/A
<b>Attack Vector</b>	Network	N/A	N/A

	Red Hat	NVD	CVE List
<b>Attack Complexity</b>	Low	N/A	N/A
<b>Privileges Required</b>	None	N/A	N/A
<b>User Interaction</b>	Required	N/A	N/A
<b>Scope</b>	Changed	N/A	N/A
<b>Confidentiality Impact</b>	Low	N/A	N/A
<b>Integrity Impact</b>	None	N/A	N/A
<b>Availability Impact</b>	None	N/A	N/A

## CVSS v3 Vector

**Red Hat:** CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

## Acknowledgements

Red Hat would like to thank Albrecht Dreß for reporting this issue.

## Frequently Asked Questions

Why is Red Hat's CVSS v3 score or Impact different from other vendors?	▼
My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?	▼
What can I do if my product is listed as "Will not fix"?	▼
What can I do if my product is listed as "Fix deferred"?	▼
What is a mitigation?	▼
I have a Red Hat product but it is not in the above list, is it affected?	▼
Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?	▼
My product is listed as "Out of Support Scope". What does this mean?	▼

**Not sure what something means?** Check out our [Security Glossary](#).

**Want to get errata notifications?** Sign up [here](#).

For clarification or corrections, please contact [Red Hat Product Security](#).

Last modified: April 23, 2026 at 12:33:45 PM UTC

CVE description copyright © 2021



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 Do Not Sell or Share My Personal Information](#)