CVE

VEX
Public o
Last mo

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

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	webkitgtk4

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
CVSS v3 Base Score	4.7	N/A	N/A
Attack Vector	Network	N/A	N/A

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