



Webkit: webkitgtk: remote user-assisted information disclosure via file drag-and-drop

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2025-13947 |
| State | PUBLISHED |
| Assigner | redhat |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2025-12-03 10:15:47 UTC |
| Updated | 2026-04-20 13:16:10 UTC |
| Description | A flaw was found in WebKitGTK. This vulnerability allows remote, user-assisted information disclosure that can reveal any f |

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from secalert@redhat.com

CVSS: 3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

Problem Types: CWE-346 | CWE-346 CWE-346 Origin Validation Error

| Version | Source | Type | Score | Severity | Vector |
|---------|---------------------|-----------|-------|----------|--|
| 3.1 | secalert@redhat.com | Secondary | 7.4 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N |
| 3.1 | CNA | CVSS | 7.4 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N |

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|--------|--------------------|---|-------------------------------|
| CNA | The WebKitGTK Team | WebKitgtk | affected 2.50.3 semver |
| CNA | Red Hat | Red Hat Enterprise Linux 7 Extended Lifecycle Support | unaffected 0:2.50.3-2.el7_9 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8 | unaffected 0:2.50.3-1.el8_10 |
| CNA | Red Hat | Red Hat Enterprise Linux 8.2 Advanced Update Support | unaffected 0:2.50.3-2.el8_2 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support | unaffected 0:2.50.3-2.el8_4 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On | unaffected 0:2.50.3-2.el8_4 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support | unaffected 0:2.50.3-2.el8_6 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8.6 Telecommunications Update Service | unaffected 0:2.50.3-2.el8_6 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8.6 Update Services For SAP Solutions | unaffected 0:2.50.3-2.el8_6 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8.8 Telecommunications Update Service | unaffected 0:2.50.3-2.el8_8 * |
| CNA | Red Hat | Red Hat Enterprise Linux 8.8 Update Services For SAP Solutions | unaffected 0:2.50.3-2.el8_8 * |
| CNA | Red Hat | Red Hat Enterprise Linux 9 | unaffected 0:2.50.3-1.el9_7 * |
| CNA | Red Hat | Red Hat Enterprise Linux 9.0 Update Services For SAP Solutions | unaffected 0:2.50.3-1.el9_0 * |
| CNA | Red Hat | Red Hat Enterprise Linux 9.2 Update Services For SAP Solutions | unaffected 0:2.50.3-1.el9_2 * |
| CNA | Red Hat | Red Hat Enterprise Linux 9.4 Extended Update Support | unaffected 0:2.50.3-1.el9_4 * |
| CNA | Red Hat | Red Hat Enterprise Linux 9.6 Extended Update Support | unaffected 0:2.50.3-1.el9_6 * |
| CNA | Red Hat | Red Hat Enterprise Linux 6 | Not specified |
| CNA | Red Hat | Red Hat Enterprise Linux 7 | Not specified |

References

| Reference | Source | Link | Tags |
|---|---------------------|---|------|
| access.redhat.com/errata/RHSA-2025:23452 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:23434 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:22790 | secalert@redhat.com | access.redhat.com | |
| bugzilla.redhat.com/show_bug.cgi | secalert@redhat.com | bugzilla.redhat.com | |
| bugs.webkit.org/show_bug.cgi | secalert@redhat.com | bugs.webkit.org | |
| access.redhat.com/errata/RHSA-2025:23583 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:22789 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:23451 | secalert@redhat.com | access.redhat.com | |

| | | | |
|---|--|---|---------------------|
| access.redhat.com/errata/RHSA-2025:23110 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:23433 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:23591 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/security/cve/CVE-2025-13947 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:23743 | secalert@redhat.com | access.redhat.com | |
| access.redhat.com/errata/RHSA-2025:23742 | secalert@redhat.com | access.redhat.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

Vendor Comments And Credit

Discovery Credit

CNA: Red Hat would like to thank Janet Black for reporting this issue. (en)

Additional Advisory Data

| Source | Time | Event |
|--------|--------------------------|----------------------|
| CNA | 2025-12-03T08:57:27.767Z | Reported to Red Hat. |
| CNA | 2025-12-03T00:00:00.000Z | Made public. |

Workarounds

CNA: Mitigation for this issue is either not available or the currently available options don't meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base or stability.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report