Bug 2418576 (CVE-2025-13947) - CVE-2025-13947 webkit: WebKitGTK: Remote user-assisted information disclosure via file drag-and-drop

Keywords: Security

Status: NEW

Alias: CVE-2025-13947

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~2418579~~ ~~2418580~~ ~~2418581~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-12-03 09:07 UTC by OSIDB Bzimport

Modified: 2025-12-22 01:53 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2025:22789	0	None	None	None	2025-12-08 01:48:15 UTC
Red Hat Product Errata	RHSA-2025:22790	0	None	None	None	2025-12-08 01:53:03 UTC
Red Hat Product Errata	RHSA-2025:23110	0	None	None	None	2025-12-11 11:34:08 UTC

Red Hat Product Errata	RHSA-2025:23433	0	None	None	None	2025-12-17 04:55:52 UTC
Red Hat Product Errata	RHSA-2025:23434	0	None	None	None	2025-12-17 06:09:58 UTC
Red Hat Product Errata	RHSA-2025:23451	0	None	None	None	2025-12-17 12:15:10 UTC
Red Hat Product Errata	RHSA-2025:23452	0	None	None	None	2025-12-17 14:00:44 UTC
Red Hat Product Errata	RHSA-2025:23583	0	None	None	None	2025-12-18 09:25:55 UTC
Red Hat Product Errata	RHSA-2025:23591	0	None	None	None	2025-12-18 09:14:53 UTC
Red Hat Product Errata	RHSA-2025:23742	0	None	None	None	2025-12-22 01:53:19 UTC
Red Hat Product Errata	RHSA-2025:23743	0	None	None	None	2025-12-22 01:39:40 UTC

OSIDB Bzimport 2025-12-03 09:07:24 UTC Description

```
This vulnerability allows a malicious website to read
arbitrary local files by abusing the file drag-and-drop
mechanism in WebKitGTK. The flaw exists because WebKitGTK does
not verify that drag operations originate from outside the
browser before granting access to the referenced file path. A
crafted webpage can prompt the user to perform an innocent-
looking drag action that unintentionally exposes sensitive
file content accessible to the user account. This results in a
remote, user-assisted information disclosure vulnerability
that can reveal any file the user is permitted to read.
```

Leonardo Taccari 2025-12-04 10:08:29 UTC Comment 2

```
Are there any further details? Which versions are affected?
Was it reported upstream?

Can you please add such details as references too when filling
```

CVEs?

Thanks!

errata-xmlrpc 2025-12-08 01:48:14 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2025:22789 https://access.redhat.com/errata/RHSA-2025:22789

errata-xmlrpc 2025-12-08 01:53:02 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2025:22790 https://access.redhat.com/errata/RHSA-2025:22790

Leonardo Taccari 2025-12-08 12:00:55 UTC Comment 5

(In reply to Leonardo Taccari from comment #2)
> Are there any further details? Which versions are affected? Was it reported
> upstream?
>
> Can you please add such details as references too when filling CVEs?
>
> Thanks!

JFTR, this is part of <https://webkitgtk.org/security/WSA-2025-0009.html> and it was fixed upstream in version 2.50.3.

It would be nice if upstream WSA can be added as a reference too.

errata-xmlrpc 2025-12-11 11:34:06 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2025:23110 https://access.redhat.com/errata/RHSA-2025:23110

errata-xmlrpc 2025-12-17 04:55:51 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2025:23433 https://access.redhat.com/errata/RHSA-2025:23433

errata-xmlrpc 2025-12-17 06:09:57 UTC Comment 10

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.4 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.4 Extended Update Support Long-Life Add-On

Via RHSA-2025:23434 https://access.redhat.com/errata/RHSA-2025:23434

errata-xmlrpc 2025-12-17 12:15:08 UTC Comment 11

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2025:23451 https://access.redhat.com/errata/RHSA-2025:23451

errata-xmlrpc 2025-12-17 14:00:43 UTC Comment 12

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2025:23452 https://access.redhat.com/errata/RHSA-2025:23452

errata-xmlrpc 2025-12-18 09:14:52 UTC Comment 13

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2025:23591 https://access.redhat.com/errata/RHSA-2025:23591

errata-xmlrpc 2025-12-18 09:25:54 UTC Comment 14

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2025:23583 https://access.redhat.com/errata/RHSA-2025:23583

errata-xmlrpc 2025-12-22 01:39:39 UTC Comment 15

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.6 Advanced Mission Critical Update Support
  Red Hat Enterprise Linux 8.6 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.6 Telecommunications Update Service

Via RHSA-2025:23743 https://access.redhat.com/errata/RHSA-2025:23743

errata-xmlrpc 2025-12-22 01:53:18 UTC Comment 16

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8.8 Update Services for SAP Solutions
  Red Hat Enterprise Linux 8.8 Telecommunications Update Service

Via RHSA-2025:23742 https://access.redhat.com/errata/RHSA-2025:23742

Note

You need to log in before you can comment on or make changes to this bug.