# Bug 2416300 (CVE-2025-13502) - CVE-2025-13502 webkit: WebKitGTK / WPE WebKit: Out-of-bounds read and integer underflow vulnerability leading to DoS

**Keywords:** Security

**Status:** NEW

**Alias:** CVE-2025-13502

**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:** ~~2416965~~ ~~2416966~~ ~~2416967~~ ~~2416968~~

**Blocks:**

**TreeView+** depends on / blocked

**Reported:** 2025-11-21 07:54 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 01:48:00 UTC |
| Red Hat Product Errata | RHSA-2025:22790 | 0 | None | None | None | 2025-12-08 01:52:47 UTC |

| | | | | | | |
|---|---|---|---|---|---|---|
| Red Hat Product Errata | RHSA-2025:23110 | 0 | None | None | None | 2025-12-11 11:33:55 UTC |
| Red Hat Product Errata | RHSA-2025:23433 | 0 | None | None | None | 2025-12-17 04:55:40 UTC |
| Red Hat Product Errata | RHSA-2025:23434 | 0 | None | None | None | 2025-12-17 06:09:46 UTC |
| Red Hat Product Errata | RHSA-2025:23451 | 0 | None | None | None | 2025-12-17 12:14:56 UTC |
| Red Hat Product Errata | RHSA-2025:23452 | 0 | None | None | None | 2025-12-17 14:00:15 UTC |
| Red Hat Product Errata | RHSA-2025:23583 | 0 | None | None | None | 2025-12-18 09:25:03 UTC |
| Red Hat Product Errata | RHSA-2025:23591 | 0 | None | None | None | 2025-12-18 09:14:41 UTC |
| Red Hat Product Errata | RHSA-2025:23742 | 0 | None | None | None | 2025-12-22 01:53:06 UTC |
| Red Hat Product Errata | RHSA-2025:23743 | 0 | None | None | None | 2025-12-22 01:39:27 UTC |

OSIDB Bzimport 2025-11-21 07:54:13 UTC Description

```
Out-of-bounds read and integer underflow vulnerability in the
GLib remote inspector server of WebKitGTK and WPE WebKit. The
WTF::SocketConnection::readMessage() function uses strlen()
over framed, peer-controlled data without constraining the
scan to the declared bodySize. If a crafted payload omits a
NUL terminator within that body, the function reads beyond the
frame boundary, causing an out-of-bounds read and UIProcess
crash (DoS). In addition, the computed messageNameLength is
not validated against bodySize before calculating
parametersSize = bodySize - messageNameLength, risking integer
underflow. A remote, unauthenticated client can trigger this
condition whenever the remote inspector server is enabled and
reachable, but the feature is primarily intended for debugging
and is disabled by default, which limits practical exposure.
```

Comment hidden (spam) Comment 1

errata-xmlrpc 2025-12-08 01:47:59 UTC Comment 2

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 01:52:46 UTC Comment 3

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

errata-xmlrpc 2025-12-11 11:33:53 UTC Comment 4

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 04:55:38 UTC Comment 7

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 06:09:44 UTC Comment 8

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 12:14:55 UTC Comment 9

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 14:00:13 UTC Comment 10

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 09:14:39 UTC Comment 11

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 09:25:01 UTC Comment 12

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 01:39:25 UTC Comment 13

```
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 01:53:05 UTC Comment 14

```
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.