Bug 2403688 (CVE-2025-11731) - CVE-2025-11731 libxslt: Type Confusion in exsltFuncResultCompfunction of libxslt

Keywords: Security

Status: NEW

Alias: CVE-2025-11731

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2403691 2403692 2403693 2403694 2403695 2403697 ~~2403696~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-10-14 05:31 UTC by OSIDB Bzimport

Modified: 2025-10-14 06:01 UTC (History)

CC List: 2 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-10-14 05:31:41 UTC Description

```
Type Confusion vulnerability in the EXSLT <func:result>
element handler of libxslt. The flaw resides in the
exsltFuncResultComp() function, which walks up the node
hierarchy to verify that a <func:result> is a descendant of a
func:function element. If no such ancestor exists, the loop
continues until the XML document node is reached, where the ns
pointer is incorrectly interpreted as integer fields
(compression and standalone). This type confusion results in
reading memory from an unexpected address, leading to a
segmentation fault or crash. Although the impact is limited to
denial-of-service, the issue can be triggered remotely by
```

```
processing malicious XSL stylesheets.
```

Note

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