Bug 2372952 (CVE-2025-6170) - CVE-2025-6170 libxml2: Stack Buffer Overflow in xmllint Interactive Shell Command Handling

Keywords: Security

Status: NEW

Alias: CVE-2025-6170

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: 2372956 2372957 2372958 2372959 2372963 2372964 2372965 ~~2372960~~ ~~2372961~~ ~~2372962~~

Blocks:

TreeView+ depends on / blocked

Reported: 2025-06-16 06:00 UTC by OSIDB Bzimport

Modified: 2026-03-24 03:52 UTC (History)

CC List: 22 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2025-06-16 06:00:53 UTC Description

```
Stack-based buffer overflow vulnerability in the interactive
shell of the xmllint tool in libxml2. The issue is caused by
an unsafe use of strcpy() when processing user-supplied
command-line input. When an attacker passes an overly long
argument to any shell command (e.g., exit, cat, etc.), the
input exceeds the fixed-size stack buffer, resulting in a
crash or potentially arbitrary code execution on systems
lacking stack protections.
This vulnerability affects only the interactive shell and
requires that an attacker can influence or control the command
```

```
input to xmllint, which is uncommon in typical deployments.
```

Note

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