Bug 2435940 (CVE-2026-1757) - CVE-2026-1757 libxml2: Memory Leak Leading to Local Denial of Service in xmllint Interactive Shell

Keywords: Security

Status: NEW

Alias: CVE-2026-1757

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2435942 2435943 2435944 2435945 2435946 2435947 2435949 ~~2435948~~

Blocks:

TreeView+ depends on / blocked

Reported: 2026-02-02 11:46 UTC by OSIDB Bzimport

Modified: 2026-02-02 12:15 UTC (History)

CC List: 18 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-02-02 11:46:33 UTC Description

```
Memory leak vulnerability in the xmllint interactive shell
command parser. The issue is caused by improper memory
management when processing input lines that consist solely of
whitespace characters. In this scenario, the allocated command
buffer is not freed before continuing execution, resulting in
a persistent memory leak. By repeatedly supplying large
whitespace-only inputs, a local attacker can cause unbounded
memory growth, eventually exhausting system resources and
triggering an out-of-memory (OOM) condition. This flaw can be
exploited without authentication but requires local access to
```

the xmllint shell, leading to a denial-of-service condition.

Note

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