



Bug 2429933 (CVE-2026-0989) - CVE-2026-0989 libxml2: Unbounded RelaxNG Include Recursion Leading to Stack Overflow

Keywords: Security

Reported: 2026-01-15 12:53 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-01-15 13:48 UTC ([History](#))

Alias: CVE-2026-0989

CC List: 18 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

- Depends On:**
- 2429936
 - 2429937
 - 2429938
 - 2429939
 - 2429940
 - 2429941
 - 2429942
 - 2429943
 - 2429944
 - 2429945
 - 2429946
 - 2429947

Blocks:

TreeView+ [depends on](#) / [blocked](#)

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-01-15 12:53:01 UTC

[Description](#)

Uncontrolled recursion vulnerability in the RelaxNG include handling logic of the libxml2 XML parsing library. The issue arises from the absence of limits on recursive <include> directive resolution. When a deeply nested chain of included RelaxNG schema files is processed, the parser enters unbounded recursion, eventually exhausting the system call stack. This results in a stack overflow and application crash. Exploitation requires attacker-controlled schema input and

primarily impacts availability by causing a denial of service.

Note

You need to [log in](#) before you can comment on or make changes to this bug.

