



Bug 2429975 (CVE-2026-0992) - CVE-2026-0992 libxml2: libxml2: Denial of Service via crafted XML catalogs

Keywords: Security ✕

Reported: 2026-01-15 13:35 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-01-15 13:47 UTC ([History](#))

Alias: CVE-2026-0992

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 DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2429976](#) [2429977](#) [2429978](#)
[2429979](#) [2429980](#) [2429981](#)
[2429982](#) [2429983](#) [2429984](#)
[2429985](#) [2429986](#) [2429987](#)

Blocks:

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

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-01-15 13:35:59 UTC

[Description](#)

Uncontrolled resource consumption vulnerability in the XML catalog processing logic of the libxml2 library. The issue arises when handling chains of XML catalogs that contain repeated <nextCatalog> elements pointing to the same downstream catalog. During entity resolution, the parser redundantly traverses catalog chains, causing exponential growth in processing time as depth increases. This can be exploited by supplying crafted catalogs to cause excessive CPU consumption and degrade application availability, resulting in

a denial-of-service condition.

Note

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

