Bug 2429959 (CVE-2026-0990) - CVE-2026-0990 libxml2: libxml2: Denial of Service via uncontrolled recursion in XML catalog processing

Keywords: Security ×

Status: NEW

Alias: CVE-2026-0990

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: 2429960 2429961 2429962 2429963 2429964 2429965 2429966 2429967 2429968 2429969 2429970 2429971

Blocks:

TreeView+ depends on / blocked

Reported: 2026-01-15 13:19 UTC by OSIDB Bzimport

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

CC List: 18 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-01-15 13:19:31 UTC Description

```
Uncontrolled recursion vulnerability in the
xmlCatalogXMLResolveURI function of the libxml2 XML parsing
library. The issue occurs when an XML catalog contains a
delegate URI entry that references the catalog itself. During
entity resolution, the function recursively resolves the same
catalog entry without detecting the cyclic reference. This
results in infinite recursion and eventual call stack
exhaustion, leading to a segmentation fault. Exploitation is
configuration-dependent and primarily impacts availability by
```

allowing an attacker to crash affected applications.

Note

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