Bug 2461300 (CVE-2026-6732) - CVE-2026-6732 libxml2: libxml2: Denial of Service via crafted XSD-validated document

Keywords:	Security	**Reported:**	2026-04-23 22:09 UTC by OSIDB Bzimport
Status:	NEW	**Modified:**	2026-04-23 22:13 UTC (History)
Alias:	CVE-2026-6732	**CC List:**	16 users (show)
Product:	Security Response	**Fixed In Version:**	
Component:	vulnerability	**Clone Of:**	
		Environment:	
Version:	unspecified	**Last Closed:**	
Hardware:	All	**Embargoed:**	
OS:	Linux		
Priority:	medium		
Severity:	medium		
Target Milestone:	---		
Assignee:	Product Security DevOps Team		
QA Contact:			
Docs Contact:			
URL:			
Whiteboard:			
Depends On:			
Blocks:			
TreeView+	depends on / blocked		

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-23 22:09:03 UTC Description

```
xmlParseReference in parser.c passes ctxt instead of ctxt-
>userData to the SAX characters / cdataBlock callbacks when
emitting the first or last text child of a cached entity tree
(parser.c). Every other SAX callsite in the same file
correctly passes ctxt->userData.

When xmlSchemaSAXPlug is active, which is the case for every
user of xmlTextReaderSetSchema / xmlTextReaderSchemaValidate
and for lxml's XMLParser(schema=...), ctxt->userData has been
swapped to a _xmlSchemaSAXPlug *. Handing the confused
charactersSplit handler a raw xmlParserCtxt * causes it to
dereference ctxt->myDoc as the forwarded SAX handler and call
myDoc->URL as a function pointer, producing a reliable SIGSEGV
on the first internal-entity reference in any XSD-validated
```

```
document. If myDoc->URL is NULL, the secondary path
(xmlSchemaSAXHandleText with a garbage plug pointer) crashes
instead.
```

Note

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