DCMTK - Bug #1214

Unbounded recursion in XMLParser library

2026-05-24 19:19 - Marco Eichelberg

Status:	Closed	**Start date:**	2026-05-24
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	2:00 hours
Target version:			
Module:	ofstd	**Compiler:**	
Operating System:			

Description

The methods XMLNode::ParseXMLElement() and XMLNode::emptyTheNode() in ofstd/libsrc/ofxml.cc recurse on the stack for each XML nesting level with no depth limit.
Reading an XML file with an extremely high nesting level (60,000 levels) triggers a stack overflow.

This can be demonstrated with the attached PoC file: dcmencap poc.xml poc.dcm

Reported 2026-05-19 by Arjun Basnet, Senior Security Researcher, Securin.

History

#1 - 2026-05-24 19:22 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 2:00 h

Closed by commit #d12e350e6.

#2 - 2026-05-25 12:01 - Marco Eichelberg

This issue has been registered as CVE-2026-44033.

#3 - 2026-05-25 12:08 - Marco Eichelberg

- Private changed from Yes to No

Files

poc.xml	1.43 MB	2026-05-24	Marco Eichelberg