DCMTK - Bug #1224

xml2dcm parseDataSet / parseSequence mutual recursion

2026-06-16 18:12 - Marco Eichelberg

Status:	Closed	**Start date:**	2026-06-16
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	1:00 hour
Target version:			
Module:	dcndata	**Compiler:**	
Operating System:			

Description

DcmXMLParseHelper::parseDataSet() at xml2dcm.cc:618 calls parseSequence() for every <sequence> element. parseSequence() at xml2dcm.cc:457 calls parseDataSet() for every `<item>` element. This mutual recursion has no depth limit. At 15,000 nested levels the default 8 MB stack is exhausted.

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

This issue has been registered as CVE-2026-44036.

History

#1 - 2026-06-16 18:15 - Marco Eichelberg

- % Done changed from 0 to 100

- Estimated time set to 1:00 h

- Private changed from No to Yes

Closed by commit #87f256d73.

#2 - 2026-06-17 17:46 - Marco Eichelberg

- Status changed from New to Closed

#3 - 2026-06-19 14:33 - Marco Eichelberg

- Private changed from Yes to No

Files

poc_007_deep.xml	879 KB	2026-06-16	Marco Eichelberg