DCMTK - Bug #1225

json2dcm readValue JSON SQ unbounded recursion

2026-06-16 18:24 - 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:	dcmdata	**Compiler:**	
Operating System:			

Description

DcmJsonReaderBase::readValue() recurses via DcmJsonReaderBase::parseSequence() on SQ JSON value items with no depth check. At 15,000 nesting levels the 8 MB default stack is exhausted.

History

#1 - 2026-06-16 18:24 - Marco Eichelberg

This issue has been registered as CVE-2026-44037.

#2 - 2026-06-16 18:25 - Marco Eichelberg

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

#3 - 2026-06-17 16:52 - Marco Eichelberg

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

- Estimated time set to 1:00 h

Closed by commit #cf955e64c.

#4 - 2026-06-19 14:33 - Marco Eichelberg

- Private changed from Yes to No

Files

poc_008_deep.json	513 KB	2026-06-16	Marco Eichelberg