DCMTK - Bug #1191

Stack Overflow via Deeply Nested DICOM Sequences

2026-03-10 21:31 - Michael Onken

Status:	Closed	**Start date:**	2026-03-10
Priority:	High	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Library	**Estimated time:**	0:00 hour
Target version:	3.7.1		
Module:	dcmdata	**Compiler:**	
Operating System:			

Description

Received by email from the IN-CYPHER OSS Security Team (2026-03-09):

> **Subject:** IC-DCMTK-0003: Stack Overflow via Deeply Nested DICOM Sequences
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-674 (Uncontrolled Recursion)
>
> This report describes a stack overflow in the
> binary DICOM parser caused by unbounded mutual recursion between
> DcmSequenceOfItems::read() and DcmItem::read(). A crafted DICOM file
> containing approximately 1,060 levels of nested sequences (using tag
> (0040,A730) Content Sequence) exhausts the call stack, crashing any
> DCMTK-based application that parses the file. The PoC is only ~40 KB and
> affects all DICOM parsing operations including dcmdump, network
> services, and PACS servers. No recursion depth limit exists anywhere in
> the call chain.
>
> Please find the detailed report, proof-of-concept, and sanitizer output
> in the attachments.

History

#1 - 2026-03-10 22:31 - Jörg Riesmeier

- Description updated

#2 - 2026-03-10 23:54 - Jörg Riesmeier

- Description updated

#3 - 2026-03-10 23:57 - Jörg Riesmeier

- Description updated

#4 - 2026-04-02 15:04 - Jörg Riesmeier

- Priority changed from Normal to High

#5 - 2026-04-04 14:45 - Michael Onken

- Status changed from New to Closed

Closed with commit 885ff0f10.

#6 - 2026-04-24 11:20 - Michael Onken

- Private changed from Yes to No

Files

IC-DCMTK-0003_poc.dcm	38.9 KB	2026-03-10	Michael Onken

IC-DCMTK-0003_crash_output.txt	40 KB	2026-03-10	Michael Onken
IC-DCMTK-0003_REPORT.md	4.97 KB	2026-03-10	Michael Onken