DCMTK - Bug #1215

Unbounded recursion in DcmDicomDir::moveRecordToTree()

2026-05-24 19:41 - 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:	dcmdata	**Compiler:**	
Operating System:			

Description

The method DcmDicomDir::moveRecordToTree() (dcmdata/libsrc/dcdicdir.cc) recurses on each child directory record without a depth limit. A maliciously crafted DICOMDIR with 10,000+ chained records exhausts the stack.

The issue can be demonstrated by compiling DCMTK with -fsanitize=address and then running the following command in a directory where the two PoC files are present: dcmmkdir --append IMAGE

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

History

#1 - 2026-05-25 11:56 - Marco Eichelberg

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

- Estimated time set to 2:00 h

Fixed by commit #ca761f7f3.

This issue has been registered as CVE-2026-44035.

#2 - 2026-06-19 14:33 - Marco Eichelberg

- Private changed from Yes to No

Files

IMAGE	1.05 KB	2026-05-24	Marco Eichelberg
DICOMDIR	742 KB	2026-05-24	Marco Eichelberg