DCMTK - Bug #1213

RLE decodeFrame() Heap-OOB Read

2026-05-23 18:02 - Marco Eichelberg

Status:	Closed	**Start date:**	2026-05-23
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmdata	**Compiler:**	
Operating System:			

Description

DcmRLECodecDecoder::decodeFrame() (dcmdata/libsrc/dcrleccd.cc:583) calls memcpy(rleHeader, rleData, 64) without validating that the pixel fragment is at least 64 bytes. The sibling decode() function has this guard at line 193 but decodeFrame() does not. An 8-byte crafted RLE fragment causes ASan to confirm a heap-buffer-overflow READ of size 64, leaking up to 56 bytes of adjacent heap memory. Affects all third-party consumers of DcmPixelData::getUncompressedFrame().

The issue can be demonstrated with the attached PoC file: dcm2img -d rle_crash.dcm rle_crash.bmp

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

History

#1 - 2026-05-23 18:05 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

Closed by commit #45469f3c3.

#2 - 2026-05-25 12:02 - Marco Eichelberg

This issue has been registered as CVE-2026-44034.

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

- Private changed from Yes to No

Files

rle_crash.dcm	682 Bytes	2026-05-23	Marco Eichelberg