DCMTK - Bug #1221

Out-of-bounds read in bundled IJG JPEG Huffman decoder

2026-06-10 11:13 - Michael Onken

Status:	Closed	**Start date:**	2026-06-10
Priority:	Normal	**Due date:**	
Assignee:	Michael Onken	**% Done:**	0%
Category:	Library	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmjpeg	**Compiler:**	
Operating System:			

Description

DCMTK's bundled IJG JPEG library (dcmjpeg/libijg8, and the identical libijg12/libijg16 copies) contains a Huffman-table validation bug that leads to an out-of-bounds read when decoding a crafted JPEG-compressed DICOM image.

The DC Huffman table validation in jdhuff.c accepts a symbol value of 16, but the extend_test[] lookup array used during coefficient decoding only has 16 valid entries (indices 0–15). A JPEG containing a DC Huffman code mapped to symbol 16 therefore causes the decoder to read one element past the end of extend_test[], a global-buffer-overflow (CWE-125). The same validation flaw triggers crashes in all three decoder variants — sequential, lossless, and progressive — and is reachable from untrusted input through any tool or application that decodes JPEG, including dcmdjpeg, dcm2img, dcmj2pnm, and anything using DJDecoderRegistration or DicomImage.

Full analysis, proof-of-concept, and a patch proposed by the original sender are in the attached report.

Thanks to Yiyi Wang for reporting this issue.

History

#1 - 2026-06-11 07:39 - Michael Onken

Fixed with commit d6ae1bc8d5b9ae9c7300013c8c85cc2ea0fd8cf5.

#2 - 2026-06-12 11:59 - Michael Onken

- Status changed from New to Closed

- Private changed from Yes to No

Files

vuln-1-ijg-jpeg-global-buffer-overflow.zip	8.41 KB	2026-06-10	Michael Onken