DCMTK - Bug #1223

Out-of-bounds read in CharLS JPEG-LS QuantizeGratient()

2026-06-10 11:16 - Michael Onken

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

Description

DCMTK's bundled CharLS JPEG-LS library (dcmjpls/libcharls) performs an out-of-bounds heap read in its near-lossless decoder (NEAR > 0) when decoding a crafted image. The gradient bounds check in DoLine() (scan.h) uses a strict > instead of >= when comparing a gradient difference against RANGE_UPPER = 1 << bpp. A gradient difference exactly equal to RANGE_UPPER therefore passes the check and reaches QuantizeGratient(), which indexes _pquant[RANGE_UPPER] — one element past the end of the dynamically-allocated quantization table, which is valid only for indices [-RANGE, RANGE-1] (CWE-125). The read is reachable from untrusted input through any tool or application that decodes near-lossless JPEG-LS, including dcmdjpls, dcm2img, dcmj2pnm, and anything using DJLSDecoderRegistration or DicomImage.

Full analysis and proof-of-concept are in the attached report.

Thanks to Yiyi Wang for reporting this issue.

History

#1 - 2026-06-11 07:40 - Michael Onken

Fixed with commit b6691c7a0fdfd261c20c2509c2ac16966bd37763

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

- Status changed from New to Closed

- Private changed from Yes to No

Files

vuln-3-charls-quantize-heap-overflow.zip	8.03 KB	2026-06-10	Michael Onken