DCMTK - Bug #1222

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

2026-06-10 11:15 - 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 when finishing decode of a crafted JPEG-LS bitstream.

DecoderStrategy::EndScan() in decodstr.h calls current_value() unconditionally after the compressed bitstream has been fully consumed, and current_value() reads (*_position)[_current_offset] with no bounds check. When a fragment is constructed so that decoding exhausts the buffer exactly, _current_offset equals the buffer length and the read goes one byte past the end of the heap allocation (CWE-125). In ASan builds this crashes the process; in production builds the adjacent heap byte is read silently and used in a branch before CharLS raises TooMuchCompressedData, so the out-of-bounds read occurs regardless. The issue is reachable from untrusted input via dcmdjpls, dcm2img, dcmj2pnm, and any application 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 - 2026-06-10 11:15 - Michael Onken

- Private changed from No to Yes

#2 - 2026-06-10 11:16 - Michael Onken

- File vuln-2-charls-endscan-heap-overflow.zip added

#3 - 2026-06-11 07:40 - Michael Onken

Fixed with commit b818c19720bd3c5c273f7c0578fef3990333af22

#4 - 2026-06-12 11:59 - Michael Onken

- Status changed from New to Closed

- Private changed from Yes to No

Files

vuln-2-charls-endscan-heap-overflow.zip	7.52 KB	2026-06-10	Michael Onken