DCMTK - Bug #1190

Infinite Loop in JPEG Segment Parser TEM Marker

2026-03-10 19:21 - Jörg Riesmeier

Status:	Closed	**Start date:**	2026-03-10
Priority:	Normal	**Due date:**	
Assignee:	Jörg Riesmeier	**% Done:**	100%
Category:	Library	**Estimated time:**	1:00 hour
Target version:	3.7.1		
Module:	dcmjpeg	**Compiler:**	
Operating System:			

Description

Received by email from the IN-CYPHER OSS Security Team (2026-03-09):

> **Subject:** IC-DCMTK-0004 Infinite Loop in JPEG Segment Parser TEM Marker
> **Version:** DCMTK master 418274445 (DCMTK-3.7.0+64)
> **CWE:** CWE-835 (Loop with Unreachable Exit Condition)
>
> This report describes a infinite loop in DJCodecDecoder::scanJpegDataForBitDepth() at djcodecd.cc:852. The function's JPEG marker parsing loop handles over 30 marker types, with each case advancing the parsing offset -- except the TEM marker (0xFF01), whose case contains only a break without incrementing the offset. This causes the parser to re-read the same TEM marker indefinitely, consuming 100% CPU with no timeout or iteration limit. A 526-byte DICOM file with a JPEG stream containing a TEM marker triggers this hang. The fix is a single line: adding offset += 2; before the break.
>
> Please find the detailed report, proof-of-concept, and sanitizer output in the attachments.

History

#1 - 2026-03-10 23:43 - Jörg Riesmeier

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 1:00 h

Closed by commit a2fef890f.

#2 - 2026-03-10 23:54 - Jörg Riesmeier

- Description updated

#3 - 2026-03-10 23:58 - Jörg Riesmeier

- Description updated

#4 - 2026-03-12 09:28 - Jörg Riesmeier

- Private changed from Yes to No

Files

IC-DCMTK-0004_poc.dcm	526 Bytes	2026-03-10	Jörg Riesmeier
IC-DCMTK-0004_crash_output.txt	913 Bytes	2026-03-10	Jörg Riesmeier
IC-DCMTK-0004_REPORT.md	2.86 KB	2026-03-10	Jörg Riesmeier