DCMTK - Bug #1211

Heap-buffer-overflow in I2DBmpSource::parse24_32BppRow()

2026-05-21 14:37 - Marco Eichelberg

Status:	Closed	**Start date:**	2026-05-21
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	1:00 hour
Target version:			
Module:	dcmdata	**Compiler:**	
Operating System:			

Description

An invalid BMP file with 16, 24 or 32 bit per pixel that contains a color palette (which is not permitted for these images) consisting only of gray values causes a buffer overflow in I2DBmpSource::parse24_32BppRow(). The code only allocated enough memory for a monochrome image, but then writes an RGB bitmap into that buffer.

The issue can be reproduced by compiling DCMTK with -fsanitize=address,undefined and then calling

```
img2dcm -i BMP oob-i2dbmps-parse24bpp.bmp out.dcm
```

Reported 2026-05-04 by Kaixuan.

History

#1 - 2026-05-21 14:44 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 1:00 h

Closed by commit #68b57d3cf.

#2 - 2026-05-25 12:10 - Marco Eichelberg

- Private changed from Yes to No

Files

oob-i2dbmps-parse24bpp.bmp	70 Bytes	2026-05-21	Marco Eichelberg