DCMTK - Bug #1099

Decoders for compressed images may segfault with very large images

2023-12-28 17:26 - Marco Eichelberg

Status:	Closed	**Start date:**	2023-12-28
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:	3.7.1+		
Module:		**Compiler:**	
Operating System:			

Description

The decoders for compressed images in DCMTK apparently do not properly check if the size of a decompressed frame, or, in the case of a multi-frame image, the size of the entire decompressed image is smaller than the maximum possible size for the PixelData attribute (2^32-2 bytes, ~ 4 GBytes). An integer overflow may occur in the calculation of the required element size that leads to an allocation of a small buffer, and in turn to a buffer overflow causing a segfault during the decompression process.

All decompression decoders in DCMTK are affected at least on some platforms:

- dcmdjpeg (for JPEG)
- dcmdrle (for RLE)
- dcmdjpls (for JPEG-LS)
- dcmdjp2k (for JPEG 2000, in the private DCMJP2K module).

The RLE and JPEG decoder are only affected when compiled as 32-bit code.

This issue is tracked as issue #1090 for the private DCMJP2K module.

History

#2 - 2024-01-02 17:50 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

Fixed by commit #31ff413f9 for the public DCMTK, and by commit #f3446c907 for the private modules.