DCMTK - Bug #696

Segmentation fault in dcmimgle when using LUTs >= 32bit

2016-10-12 11:12 - Jan Schlamelcher

Status:	Closed	**Start date:**	2016-10-12
Priority:	High	**Due date:**	
Assignee:	Jörg Riesmeier	**% Done:**	100%
Category:	Library	**Estimated time:**	0:00 hour
Target version:	3.6.1+		
Module:	dcmimgle	**Compiler:**	
Operating System:	32-bit		

Description

Lines like const unsigned long ocnt = OFstatic_cast(unsigned long, inter->getAbsMaxRange()); in DiMonoOutputPixelTemplate (dcmtk/dcmimgle/dimoopxt.h) limit the number of LUT entries to what is representable by an unsigned long (Uint32 in most cases). These lines should be identified and changed to size_t instead.

History

#1 - 2016-10-12 13:48 - Jörg Riesmeier

I don't think that changing the data type is a proper solution to this issue. An array with more than 4.2 billion entries is certainly not desirable - at least not for optimization purposes.

#2 - 2016-10-18 10:12 - Jan Schlamelcher

- File overflow_696.patch added

#3 - 2016-11-30 18:17 - Jörg Riesmeier

- Status changed from New to Closed

- Assignee changed from Thorben Hasenpusch to Jörg Riesmeier

- % Done changed from 0 to 100

- Operating System set to 32-bit

Fixed with commit a8cf5d1.

Files

overflow_696.patch	10.4 KB	2016-10-18	Jan Schlamelcher