DCMTK - Bug #793

overflow error in calculation of decompressed image size

2017-09-28 15:14 - Marco Eichelberg

Status:	Closed	**Start date:**	2017-09-28
Priority:	High	**Due date:**	
Assignee:	Michael Onken	**% Done:**	0%
Category:	Library	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmdata	**Compiler:**	
Operating System:			

Description

DcmPolymorphOBOW::createUint16Array() can create an array of incorrect size when a parameter is passed that would cause the creation of a buffer larger than 4 GBytes. The first parameter to this method is numWords, the number of 16-bit words to be allocated, as a Uint32 parameter. This means that it is possible to pass a value > 2^31, which would correspond to a buffer size > 4 GByte, which is not permitted in DICOM.

This is not properly checked in the call to createEmptyValue() in dcmdata/libsrc/dcvrpobw.cc:185, and in that case a buffer that is too small is silently allocated.

The problem can be demonstrated by running dcmj2pnm +Fa +op -O <infile> <outfile> on the sample file provided in /share/dicom/contrib/20170928_large_multiframe_confidential/A000

History

#1 - 2017-12-07 11:43 - Marco Eichelberg

- Assignee set to Michael Onken

#2 - 2018-02-05 18:41 - Jan Schlamelcher

- Target version changed from 3.6.3 to 3.6.6

#3 - 2018-03-02 13:51 - Michael Onken

Closed by commit ebbc9e.

#4 - 2018-03-02 13:52 - Michael Onken

- Status changed from New to Closed

#5 - 2020-05-25 13:29 - Michael Onken

- Target version deleted (3.6.6)