

DCMTK - Bug #8

Multiple integer underflows in dcmnet/libsrc/dulparse.cc

2009-10-01 00:00 - Uli Schlachter

Status:	Closed	Start date:	
Priority:	High	Due date:	
Assignee:		% Done:	100%
Category:		Estimated time:	0:00 hour
Target version:		Compiler:	
Module:	dcmnet		
Operating System:			
Description			
Siehe Mail von Uli Schlachter vom 01.10.09 dulparse.cc "glaubt" den Längenfeldern, die die Gegenseite sendet. An vielen Stellen wird die "Rest-Länge" eines Objektes berechnet durch z.B. //pduLength -= itemLength;//. Dies kann für Integer underflows ausgenutzt werden (itemLength größer als pduLength), wodurch dcmnet dann versucht weit über das Ende des PDUs zu lesen. Beispielsweise kann man am Ende von dulconst.cc "constructPresentationContext()" folgende Zeile einfügen: <pre>context->length = 3;</pre> Alle SCUs und SCPs mit denen man nun presentation contexts aushandelt stürzen ab.			

History

#1 - 2014-09-22 16:52 - Michael Onken

- Description updated
- Private changed from No to Yes

#2 - 2015-01-15 13:39 - Michael Onken

- Private changed from Yes to No

#3 - 2016-12-14 18:03 - Marco Eichelberg

- Subject changed from Mehrere Integer underflows in dcmnet/libsrc/dulparse.cc to Multiple integer underflows in dcmnet/libsrc/dulparse.cc

This bug is also discussed in the following announcement: <http://forum.dcmthk.org/viewtopic.php?f=1&t=4498>