DCMTK - Bug #1228

Heap overflow when computing PDU length + safety margin

2026-06-19 13:09 - Michael Onken

Status:	Closed	**Start date:**	2026-06-19
Priority:	High	**Due date:**	
Assignee:	Michael Onken	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:			
Module:	dcmnet	**Compiler:**	
Operating System:			

Description

Fix potential heap overflow that could occur if the safety margin of 100 bytes added to the expected PDU length goes beyond the size of int, leading (through the sign flipping) to very large allocations.

The fix ensures that the buffer length (including safety margin) works and if larger than max PDU size (~4 GB), rejects the PDU.

Thanks to Dominik Blain for the report.

History

#1 - 2026-06-19 14:25 - Michael Onken

Fixed with commit 537815.

#2 - 2026-06-26 07:56 - Michael Onken

- Status changed from New to Closed

- Private changed from Yes to No