DCMTK - Bug #1229

Heap Overflow in DB_DuplicateElement (dcmqrdb)

2026-06-19 13:16 - 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:	dcmqrdb	**Compiler:**	
Operating System:			

Description

Using an int instead of size_t for computing the size of a buffer can make the int overflow and therefore create a much smaller buffer than actually needed.

Fix: Use a size_t cast (not int) for the malloc size so large ValueLength values can no longer truncate/sign-flip into an undersized buffer. Also run memset/memcpy only after the NULL check, avoiding a crash when the allocation fails.

Thanks to Dominik Blain for the report.

History

#1 - 2026-06-19 14:23 - Michael Onken

Fixed with commit b2d33e.

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

- Status changed from New to Closed

- Private changed from Yes to No