

DCMTK - Bug #1026

dcmqrscp may crash when reading malformed configuration file

2022-05-24 11:17 - Marco Eichelberg

Status:	Closed	Start date:	2022-05-24
Priority:	Normal	Due date:	
Assignee:	Marco Eichelberg	% Done:	100%
Category:	Library and Apps	Estimated time:	1:00 hour
Target version:	3.6.8	Compiler:	
Module:	dcmqrscp		
Operating System:			
Description			
Three issues have been detected in class DcmQueryRetrieveConfig that may cause an application crash of dcmqrscp when reading a malformed configuration file, due to insufficient validation of the input data. The issues can be reproduced by compiling DCMTK (on Linux, with gcc) using the following cmake options:			
<pre>cmake -G"Unix Makefiles" .. -DCMAKE_C_FLAGS="-g -fprofile-arcs -ftest-coverage -fsanitize=address" -DCMAKE_CXX_FLAGS="-g -fprofile-arcs -ftest-coverage -fsanitize=address"</pre>			
and then running dcmqrscp -c bugN_dcmqrscp.cfg with one of the three configuration files provided below.			
Reported 2022-05-24 by Zahra Mirzamomen < zahra.mirzamomen@monash.edu > and Marcel Böhme < marcel.boehme@mpi-sp.org >.			

History

#1 - 2022-05-24 11:24 - Marco Eichelberg

- Status changed from New to Closed
- Assignee set to Marco Eichelberg
- % Done changed from 0 to 100
- Estimated time set to 1:00 h

Fixed by commit #957fb31e5.

Files

bug1_dcmqrscp.cfg	2.31 KB	2022-05-24	Marco Eichelberg
bug2_dcmqrscp.cfg	2.36 KB	2022-05-24	Marco Eichelberg
bug3_dcmqrscp.cfg	261 Bytes	2022-05-24	Marco Eichelberg