

DCMTK - Bug #1114

Segmentation fault while receiving invalid message

2024-03-13 17:14 - Marco Eichelberg

Status:	Closed	Start date:	2024-03-13
Priority:	Normal	Due date:	
Assignee:	Marco Eichelberg	% Done:	100%
Category:	Library and Apps	Estimated time:	0:00 hour
Target version:	3.6.9	Compiler:	
Module:	dcmnet, dcmdata		
Operating System:			

Description

The dcmnet module may produce a segmentation fault due to a de-referenced NULL pointer while processing an invalid incoming DIMSE message.

Two places in the code are affected. The bugs can be reproduced as follows:

```
# Start the server
DCMDICTPATH=dicom.dic dcmrecv --config-file storescp.cfg Default -d 6789

# Trigger the bug
cat <input-hash> | nc 127.0.0.1 -p 6789
```

All required files are attached below.

Reported 2024-03-14 by Nils Bars <nils.bars@rub.de>.

History

#1 - 2024-03-18 17:00 - Marco Eichelberg

- % Done changed from 0 to 100
- Private changed from Yes to No

Closed by commit #c78e434c0.

#2 - 2024-04-12 14:36 - Marco Eichelberg

- Status changed from New to Closed

Closed by commit #c78e434c0.

Files

dicom.dic	253 KB	2024-03-13	Marco Eichelberg
storescp.cfg	33.1 KB	2024-03-13	Marco Eichelberg
063c0affa01105480bb591eaa099c6536271bde4	16.8 KB	2024-03-13	Marco Eichelberg
e46e52126c03c2e5fc518b166c3adecb1d01de41	16.5 KB	2024-03-13	Marco Eichelberg