DCMTK - Bug #1217

AE_6/AE_3 error-return paths skip heap cleanup

2026-05-27 09:33 - Michael Onken

Status:	Closed	**Start date:**	2026-05-27
Priority:	High	**Due date:**	
Assignee:	Michael Onken	**% Done:**	0%
Category:		**Estimated time:**	0:00 hour
Target version:			
Module:	dcmnet	**Compiler:**	
Operating System:			

Description

Bug as reported by Abhinav Agarwal:

Root cause: AE_6_ExamineAssociateRequest (dulfsm.cc:1231): after parseAssociate() succeeds, translatePresentationContextList() fails on a zero-TS presentation context; the error return skips cleanup at lines 1258-1259. All PRV_PRESENTATIONCONTEXTITEM nodes, transferSyntaxList sub-chains, SCUSCPRoleList, and userInfo are leaked. Distinct from Finding 2: here cleanup is never called; in Finding 2 it is called but internally broken. Fixing one does not fix the other. AE_3 (SCU-side) has the same pattern at dulfsm.cc:1010/1018.

Reproduced with: A-ASSOCIATE-RQ with 127 normal contexts + 1 zero-TS trigger. storescp --single-process: 525 connections → 256 MB heap → SIGKILL (exit -9); ~16 seconds; ~162 KB/conn. Monotonic growth also confirmed via 5,000-conn run reaching 1.2 GB RSS. AE_3: 30/30 echoscu connections against rogue SCP triggered error 0006:0318.

Scope: SCP-side: storescp, wlmscpfs, dcmqrscp. SCU-side: storescu, echoscu, findscu, movescu, getscu. wlmscpfs/dcmqrscp default to --fork on POSIX (mitigated for parent process).

Source:
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmnet/libsrc/dulfsm.cc#L1175-L1267 (AE_6 — leak at 1231, cleanup at 1258-1259 skipped)
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmnet/libsrc/dulfsm.cc#L916-L1061 (AE_3 — leak at 1010, 1018)

History

#1 - 2026-05-27 09:35 - Michael Onken

- Assignee set to Michael Onken

#2 - 2026-05-27 09:35 - Michael Onken

- Priority changed from Normal to High

#3 - 2026-05-29 18:06 - Michael Onken

A second leak was discovered during fixing the orginally reported one.

translatePresentationContextList() also now frees the proposed transfer syntax list of a rejected context. Add a dcmnet regression test (tassocleak.cc) has been added that exercises the code path through both leaks (uso Cmake option DCMTK_WITH_SANITIZERS to verify leak is gone, or use a tool like valgrind).

Fixed in commit 2312891.

#4 - 2026-05-29 18:06 - Michael Onken

- Status changed from New to Closed

#5 - 2026-06-05 11:49 - Michael Onken

- Private changed from Yes to No