DCMTK - Bug #1216

destroyUserInformationLists() leaks ExtNeg sub-items

2026-05-27 09:32 - 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: helpers.cc:67 does `delete userInfo->extNegList` which frees the OFList container but never iterates members. SOPClassExtendedNegotiationSubItem objects and their serviceClassAppInfo buffers are permanently orphaned. The correct cleanup (deleteListMembers in extneg.cc:26-36) is only called on the success path.

Reproduced with: A-ASSOCIATE-RQ with 10,911 valid 0x56 items + 1 truncated 5-byte trigger. parseExtNeg() fails at dulparse.cc:826 (availData < 6). storescp --single-process (default mode): 238 connections → 256 MB cumulative heap → SIGKILL (exit -9); post-attack C-ECHO: REFUSED; ~1.0 second at 254 conn/s; ~862 KB/conn. (256 MB limit via memory-capping harness; the bug causes monotonic growth at any limit.)

Scope: Any long-lived dcmnet SCP. storescp defaults to single-process. Fork mode mitigates (child exit reclaims).

Source:
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmnet/libsrc/helpers.cc#L54-L73 (leak — line 67)
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmnet/libsrc/dulparse.cc#L820-L857 (trigger — parseExtNeg)
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmnet/libsrc/extneg.cc#L26-L36 (correct cleanup — never called on error path)

History

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

- Priority changed from Normal to High

#2 - 2026-05-29 14:25 - Michael Onken

- Status changed from New to Closed

Fixed with commit 23f181.

#3 - 2026-06-05 11:49 - Michael Onken

- Private changed from Yes to No