

DCMTK - Bug #1248

Remote memory leak in N-GET-RQ AttributeIdentifierList handling

2026-07-14 20:58 - Michael Onken

Status:	Closed	Start date:	2026-07-14
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:		Estimated time:	0:00 hour
Target version:		Compiler:	All
Module:	dcmnet		
Operating System:	All		

Description

As reported by Eneshan Erdoğan Karaca (BoxStrike Team):

Summary

A remote, unauthenticated memory leak exists in DCMTK's DIMSE-N N-GET handling. When an SCP receives an N-GET-RQ carrying an Attribute Identifier List (0000,1005) with at least one entry, the heap buffer allocated for that list in `getAttributeList()` (`dcmnet/libsrc/dimcmd.cc`) is never freed. Repeated requests accumulate leaked memory until the SCP process is exhausted (denial of service).

Root cause

`getAttributeList()` allocates the list with `malloc` and stores it in the `AttributeIdentifierList` field of the parsed `T_DIMSE_N_GetRQ`. That struct is part of a stack `T_DIMSE_Message` that has no destructor and is reused for every command, so the pointer is lost on the next receive. The two in-tree consumers both read the list and return without freeing it:

- `DcmSCP::receiveNGETRequest()` (`dcmnet/libsrc/scp.cc`)
- `DVPSPrintSCP N-GET handling` (`dcmpstat/libsrc/dvpsprt.cc`), used by `dcmprscp`

A tree-wide search finds no `free()` for this buffer.

Impact

- Type: heap memory leak -> denial of service
- Vector: network, no authentication beyond a DICOM association
- Each N-GET-RQ with a non-empty list leaks (`ListCount * 2 + 1`) bytes

Confirmation

Reproduced by the reporter against `dcmprscp`, and confirmed here by driving `DIMSE_parseCmdObject()` under `valgrind`: the buffer is reported "definitely lost" with stack `malloc -> parseNGetRQ -> DIMSE_parseCmdObject`.

Fix

Free the Attribute Identifier List once it has been consumed, in both N-GET receive paths.

History

#1 - 2026-07-15 10:15 - Michael Onken

- Status changed from New to Closed

Fixed with commit bcf5a99aa1f2e68684ff1cf0c63d2960df7664a5.