DCMTK - Bug #1144

DiScaleTemplate<>::interpolatePixel() segfault on MacOS ARM

2024-12-25 12:37 - Marco Eichelberg

Status:	Closed	**Start date:**	2024-12-25
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:		**Compiler:**	Apple clang 15.0.0
Operating System:	MacOS		

Description

DCMTK's image scaling routine causes segmentation faults in certain situations on MacOS X ARM.
The segmentation fault EXC_BAD_ACCESS (SIGSEGV) is caused by an access to an invalid or out-of-bounds address in memory, in the following method:

```
DiScaleTemplate<unsigned char>::interpolatePixel(unsigned char const**, unsigned char**)
```

Notes:

- The error only occurs in a Release build (which uses the -O3 flag). It does **not** occur in a Debug build or a "ReleaseWithDebInfo" build (which uses -O2 -g).
- The error only occurs if interpolation algorithm 1 (--interpolate 1) is used, which is the default.

Build environment:

- Apple clang version 15.0.0 (clang-1500.0.40.1)
- Target: arm64-apple-darwin22.5.0

The issue can be reproduced with the following command line and the sample file provided here:

```
dcmscale -v --scale-x-size 800 smpte.dcm output.dcm
```

History

#1 - 2025-04-23 13:02 - Marco Eichelberg

- Status changed from New to Closed

- Compiler set to Apple clang 15.0.0

Apparently a compiler bug. Disappeared after update to Apple clang 16.0.0.

Files

smpte.dcm	257 KB	2024-12-25	Marco Eichelberg