DCMTK - Bug #1218

wlmscpfs unchecked DcmElement* to DcmSequenceOfItems* cast

2026-05-27 09:34 - 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

Root cause: wldsfs.cc has 3 functions with unchecked C-style casts of findAndGetElement() results to DcmSequenceOfItems*. With Explicit VR TS (default), attacker sends wire VR=LO for a dictionary-SQ tag like (0008,1110); dcmdata creates DcmLongString instead. Unchecked cast followed by virtual dispatch causes SIGSEGV — DcmLongString's vtable is shorter than DcmSequenceOfItems'. Same root cause as CVE-2024-28130 (dcmpstat); the fix (dc6a2446, 601b227ee) did not touch dcmwlm/.

Reproduced with: C-FIND with tag (0008,1110) VR=LO length=0. --single-process: one PDU kills the entire daemon (A:H). --single-process is a documented mode (wlmscpfs.man:66-67), common in containerized deployments; on platforms without HAVE_FORK it is the only mode. Fork mode (default on POSIX/Windows): child crashes, parent survives (A:L). Fork saturation test: 30 threads × 60s, 6,141 crash PDUs; 78/78 legitimate queries succeeded. Conservative alternate: A:L = 5.3 for fork-mode-only scoring.

Scope: wlmscpfs only. Requires Explicit VR TS (default) + ≥1 .wl record on disk. RCE ruled out.

Source:
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmwlm/libsrc/wldsfs.cc#L225-L240 (primary cast site — line 229)
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmwlm/libsrc/wldsfs.cc#L175-L195 (secondary cast site)
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmwlm/libsrc/wldsfs.cc#L353-L360 (tertiary cast site — nested cast chain)

History

#1 - 2026-05-27 09:34 - 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 14:29 - Michael Onken

Fixed in commit f4e007468.

#4 - 2026-05-29 14:31 - Michael Onken

- Status changed from New to Closed

#5 - 2026-05-29 14:40 - Michael Onken

Bug reported by Abhinav Agarwal.

#6 - 2026-06-05 11:48 - Michael Onken

- Private changed from Yes to No