# DCMTK - Bug #1210

## wlmscpfs Called AE Title used as directory path unsanitized

2026-05-20 08:17 - Michael Onken

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | 2026-05-20 |
| **Priority:** | Normal | **Due date:** | |
| **Assignee:** | Michael Onken | **% Done:** | 100% |
| **Category:** | Application | **Estimated time:** | 0:00 hour |
| **Target version:** | | | |
| **Module:** | dcmwlm | **Compiler:** | |
| **Operating System:** | | | |

**Description**

As reported by Abhinav Agarwal:

Root cause: Called AE Title from A-ASSOCIATE-RQ is concatenated directly onto dfPath at wlfsim.cc:175. No character validation. DICOM AE VR allows "/" and "." — "../VICTIM" is a conformant payload. No sanitization exists anywhere in the dcmwlm path from wire to filesystem.

Reproduced with: AET "../secret/VICTIM" (16 bytes) → association accepted, C-FIND returns all .wl records from outside dfPath. Multi-AET demo: "../CARDIOLOGY" retrieves records from a storage area the requester was not intended to access. Write primitive (non-default): with --request-file-path and --request-file-format '#c.dump', the same AET is substituted into the output filename; live demo wrote reqFilePath/../secret/VICTIM.dump outside reqFilePath. wlmactmg.cc:478-483 refuses unsupported AETs (AET acts as access gate), but no Calling AE authorization is enforced.

CVSS: 8.2 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N). I:L from confirmed write primitive (--request-file-path, documented option). Conservative alternate: I:N = 7.5 for default read-only configuration.

Scope: wlmscpfs deployments with sibling AET directories. Requires target dir with lockfile and .wl records.

Source:
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmwlm/libsrc/wlfsim.cc#L158-L183
(unsanitized concat at line 175)
https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmwlm/libsrc/wlmactmg.cc#L478-L483 (AET gate)

### History

**#1 - 2026-05-20 08:18 - Michael Onken**

*- % Done changed from 0 to 100*

Fixed with commit e3878daf870cd2db50eadfde38615f0afae8a584.

**#2 - 2026-05-20 08:18 - Michael Onken**

*- Private changed from No to Yes*

**#3 - 2026-05-25 12:15 - Marco Eichelberg**

*- Status changed from New to Closed*

*- Private changed from Yes to No*