DCMTK - Bug #1207

Filename sanitation for DcmSCU/getscu's bit preserving mode

2026-05-12 08:51 - Michael Onken

Status:	Closed	**Start date:**	2026-05-12
Priority:	Normal	**Due date:**	
Assignee:	Michael Onken	**% Done:**	0%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmnet	**Compiler:**	
Operating System:			

Description

Report from Abhinav Agarwal:

- Root cause: handleCGETSession() at scu.cc:1221-1226 passes raw AffectedSOPInstanceUID to combineDirAndFilename() without sanitizeFilename(). The parallel DISK mode path at scu.cc:1431 DOES call sanitizeFilename(). Incomplete remediation of CVE-2022-2120 — the f06a867 patch missed this branch.

- Reproduced with: getscu --bit-preserving -od /tmp/out connects to malicious C-GET SCP. SCP sends C-STORE sub-ops with UID "../../tmp/pwned" (traversal) and "/tmp/abs" (absolute override). 4 files written in one session; -od stays empty; getscu exits 0 with no warning. SSH account-takeover chain validated: traversal writes a DICOM file embedding an ed25519 public key at byte 717; when placed as authorized_keys in a test .ssh/ dir, sshd (StrictModes yes) accepted the key at line 3 and granted shell access (id captured). Negative control: same payloads without +B stay inside -od.

- CVSS: 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). DCMSCU_STORAGE_BIT_PRESERVING is a first-class documented library API (scu.h:56-67); a minimal noninteractive C++ client enables it with one method call. CVE-2022-2120 (same pattern, storescu +B) was scored AC:L/9.8 by NVD. Conservative alternate: AC:H = 8.1.

Scope: getscu (+B). Any DcmSCU consumer using DCMSCU_STORAGE_BIT_PRESERVING.

Source:

- https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmnet/libsrc/scu.cc#L1221-L1226 (vulnerable — no sanitize)
- https://github.com/DCMTK/dcmtk/blob/ccfd10b84ff3c9a40b7b331698aedf06d421fc43/dcmnet/libsrc/scu.cc#L1428-L1434 (patched sibling — has sanitize)

History

#1 - 2026-05-12 08:52 - Michael Onken

- Private changed from No to Yes

#2 - 2026-05-12 08:54 - Michael Onken

- Status changed from New to Closed

- Private changed from Yes to No

Fixed with cmomit eca9a03dd.