DCMTK - Bug #1194

OS command injection vulnerability in storescp --exec-on-reception

2026-03-14 17:40 - Marco Eichelberg

Status:	Closed	**Start date:**	2026-03-14
Priority:	High	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Application	**Estimated time:**	4:00 hours
Target version:	3.7.1		
Module:	dcmnet	**Compiler:**	
Operating System:			

Description

Three placeholder tokens used in the shell command execution feature (#f , #p , #r) are derived from attacker-controlled input with insufficient or no sanitization. An unauthenticated attacker can achieve remote code execution by sending a single crafted DICOM C-STORE request to a storescp instance configured with --exec-on-reception.

The vulnerability exists because shell metacharacters in attacker-controlled DICOM fields are not sanitized before being passed to /bin/sh -c . The DCMTK team partially addressed this class of issue in February 2024 (DCMTK issue #1109) by adding allowlist sanitization for AE title placeholders (#a , #c), but the same fix was not applied to the filename (#f), path (#p), or reverse DNS (#r) placeholders.

Reported 2026-02-21 by Machine Spirits UG (haftungsbeschränkt), contact@machinespirits.de

History

#1 - 2026-03-21 18:23 - Marco Eichelberg

This vulnerability only affects the storescp command line tool, not the underlying libraries. The vulnerability is only present when storescp is executed with either the --exec-on-reception (short form: -xcr) or the --exec-on-eostudy (short form: -xcs) command line option. It can be exploited by an attacker that is able to use a DICOM Storage Service Class SCU (such as storescu) to send maliciously manipulated DICOM objects to the affected storescp instance. The following fields can be abused by including (forbidden) shell escape characters:

- SOP Instance UID (if '#f' placeholder is present in the string passed to the execution option)
- Study Instance UID (if '#p' placeholder is present in the string passed to the execution option and the --sort-on-study-uid (short: -su) option is also in use)
- Patient Name (if '#p' placeholder is present in the string passed to the execution option and the --sort-on-patientname (short: -sp) option is also in use)
- DNS name of the SCU (if '#r' placeholder is present and the attacker is able to modify the DNS entry for the attacking system)

#2 - 2026-03-21 18:35 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 4:00 h

Closed by DCMTK commit #edbb085e4.

#3 - 2026-03-24 09:21 - Marco Eichelberg

Also see: https://machinespirits.com/advisory/2e1627/

#4 - 2026-04-07 10:33 - Marco Eichelberg

- Private changed from Yes to No

This issue has been assigned CVE number CVE-2026-5663 (https://vuldb.com/vuln/355486).