DCMTK - Bug #1109

Security vulnerability in storescp's --exec-on-reception and --exec-on-eostudy options

2024-02-21 12:35 - Marco Eichelberg

Status:	Closed	**Start date:**	2024-02-21
Priority:	High	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Application	**Estimated time:**	2:00 hours
Target version:	3.6.9		
Module:	dcmnet	**Compiler:**	
Operating System:			

Description

When storescp is executed with the --exec-on-reception or --exec-on-eostudy option, a command line can be specified that will be executed after the receipt of an image, or the receipt of an entire study, respectively.
The command line can contain certain placeholders, such as #f for the filename of the DICOM file, #a for the calling aetitle, or #c for the called aetitle.
The code that copies the application entity titles into the command line is not protected against shell escape characters. This can be abused by a malicious attacker to pass a short command (less than 16 characters) in the aetitle that will be executed by storescp.
The issue can be demonstrated by running (in two different shells):

```
storescp --exec-on-reception "echo '#c'" 10004
storescu localhost 10004 testfile.dcm --call "';touch TEST'"
```

This will cause a file named TEST" to be created in the directory where storescp is executed.

Note: This vulnerability is only present when storescp is executed with the --exec-on-reception or --exec-on-eostudy option, **and** the command line passed to this option contains the '#a' or '#c' placeholder.

Reported 2024-02-14 by Phileas Lebada <phileas@contextflow.com>.

History

#1 - 2024-02-21 12:39 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 2:00 h

Closed by commit #b789e34e1.

#2 - 2024-02-21 12:39 - Marco Eichelberg

- Private changed from No to Yes

#3 - 2024-02-25 11:44 - Marco Eichelberg

- Private changed from Yes to No