DCMTK - Bug #1021

Path traversal vulnerability in DCMTK

2022-05-06 14:02 - Marco Eichelberg

Status:	Closed	**Start date:**	2022-05-06
Priority:	High	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	6:00 hours
Target version:			
Module:		**Compiler:**	
Operating System:			

Description

Several DCMTK tools use attributes of messages or datasets received over the network to generate a filename. For example, storescp by default generates a filename consisting of a few letters representing the modality, such as "CT", followed by a period "." and the SOP Instance UID. The problem is that the SOP Instance UID is not checked for validity, so an attacker can embed arbitrary characters here, in particular something like "/../../../etc/passwd", which under certain conditions can cause a file to be written to a different directory than the working directory of storescp, with the access rights of the user executing storescp ("path traversal"). The file written is still a DICOM file, but there are file formats such as PHP that ignore arbitrary leading bytes and still find and execute content that might be embedded in a DICOM text attribute if, for example a PHP script of a web server running on the same machine is overwritten.

- Affected DCMTK tools are: storescp, movescu, getscu, dcmrecv.
- Affected private modules are: dcmppscu, dcmpps, dcmppsmg, stcomscu and dcmprscp.

Thanks to Sharon Brizinov <sharon.b@claroty.com> and Noam Moshe for the bug report and sample file and scripts.

History

#1 - 2022-05-07 12:16 - Marco Eichelberg

- Status changed from New to Closed

- % Done changed from 0 to 100

- Estimated time set to 6:00 h

Closed by commit #7e631e94b for DCMTK and commit #e1c1d069b for the private modules.

#2 - 2023-06-22 09:03 - Marco Eichelberg

Apparently the merge into the master repository has changed the commit ID. You can now find the fix as commit f06a86751.