DCMTK - Bug #858

Buffer overflow in DcmRLEDecoder::decompress()

2018-11-28 10:12 - Marco Eichelberg

Status:	Closed	**Start date:**	2018-11-28
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmdata	**Compiler:**	
Operating System:			

Description

As a part of medical infrastructure security research, the DeteAct Team started to perform fuzzing of various open source medical data processing libraries.
During fuzzing of the dcm2pnm utility, a memory corruption (buffer overflow) bug was found, which occurs in DcmRLEDecoder::decompress() (file dcrledec.h, line 122). Attached are three sample files that trigger the (same) bug when processed with either dcm2pnm or dcmdrle.

Reported 2018-11-27 by Omar Ganiev <beched@deteact.com>, DeteAct Team, Open Medical Infrastructure Security Project.

History

#1 - 2018-11-28 10:16 - Marco Eichelberg

- File dcm2pnm_case_1 added

- File dcm2pnm_case_2 added

- File dcm2pnm_case_3 added

#2 - 2018-11-28 10:38 - Marco Eichelberg

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

Closed by commit #40917614e.

#3 - 2020-05-25 13:29 - Michael Onken

- Target version deleted (3.6.6)

#4 - 2024-10-15 09:42 - Marco Eichelberg

- Status changed from Closed to Reopened

According to a report, the bug is still present if pixel data is accessed frame-by-frame:

The DcmRLEDecoder::decompress() function is fixed when called from the DcmRLECodeDecoder::decode() function, but not when called from the DcmRLECodeDecoder::decompress() function. When I try to load an image using the DcmPixelData::getUncompressedFrameSize() function, a buffer overflow occurs in the DcmRLEDecoder::decompress() function.

Reported 2024-10-15 by Kosuke Yoshinaga <kosuke.yoshinaga@goodmankk.com>.

#5 - 2024-11-13 18:06 - Marco Eichelberg

- Status changed from Reopened to Closed

Closed by commit #f93cf77f1.

Files

dcm2pnm_case_1	7.61 KB	2018-11-28	Marco Eichelberg
dcm2pnm_case_2	7.61 KB	2018-11-28	Marco Eichelberg