DCMTK - Bug #836

Buffer overflow in DcmPresentationState::createFromImage

2018-06-15 11:44 - Marco Eichelberg

Status:	Closed	**Start date:**	2018-06-15
Priority:	Normal	**Due date:**	
Assignee:	Marco Eichelberg	**% Done:**	100%
Category:	Library and Apps	**Estimated time:**	0:00 hour
Target version:			
Module:	dcmpstat	**Compiler:**	
Operating System:			

Description

The following buffer overflow can be reproduced by with the attached sample file.
It is most likely caused by an unchecked typecast.

```
Summary: global-buffer-overflow
OS: CentOS 7 64bit
Version: commit 5f22e71e6ab1654e0ca787f2d779b0a69944feef
 Steps to reproduce:
 1.Download the .POC files.
 2.Compile the source code with ASan.
 3.Execute the following command
     : ./dcmpsmk $FILE /dev/null

==3175== Jump to the invalid address stated on the next line
==3175==    at 0x68744F6D63443132: ???
==3175==    by 0x4A3FE5: DcmPresentationState::createFromImage(DcmItem&, DVPSoverlayActivation, DV
PSVOIActivation, bool, bool, bool, DVPSGraphicLayering, char const*, char const*, char const*) (dc
mpstat.cc:884)
==3175==    by 0x48B546: main (dcmpsmk.cc:303)
==3175==  Address 0x68744f6d63443132 is not stack'd, malloc'd or (recently) free'd
==3175==
==3175==
==3175== Process terminating with default action of signal 11 (SIGSEGV)
==3175==  Bad permissions for mapped region at address 0x68744F6D63443132
==3175==    at 0x68744F6D63443132: ???
==3175==    by 0x4A3FE5: DcmPresentationState::createFromImage(DcmItem&, DVPSoverlayActivation, DV
PSVOIActivation, bool, bool, bool, DVPSGraphicLayering, char const*, char const*, char const*) (dc
mpstat.cc:884)
==3175==    by 0x48B546: main (dcmpsmk.cc:303)
==3175==
```

```
=================================================================
==2532==ERROR: AddressSanitizer: global-buffer-overflow on address 0x0000009c9fd0 at pc 0x0000005b
9d2d bp 0x7fffb06db890 sp 0x7fffb06db888
READ of size 8 at 0x0000009c9fd0 thread T0
    #0 0x5b9d2c in DcmPresentationState::createFromImage(DcmItem&, DVPSoverlayActivation, DVPSVOIA
ctivation, bool, bool, bool, DVPSGraphicLayering, char const*, char const*, char const*) /home/kar
as/dcmtk/dcmpstat/libsrc/dcmpstat.cc:884:16
    #1 0x574522 in main /home/karas/dcmtk/dcmpstat/apps/dcmpsmk.cc:303:19
    #2 0x7f5d9939a1c0 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x211c0)
    #3 0x47aa29 in _start (/home/karas/dcmtk/bin/dcmpsmk+0x47aa29)

0x0000009c9fd0 is located 0 bytes to the right of global variable 'vtable for DcmOtherByteOtherWor
d' defined in '/home/karas/dcmtk/dcmdata/libsrc/dcvrobow.cc' (0x9c9ce0) of size 752
SUMMARY: AddressSanitizer: global-buffer-overflow /home/karas/dcmtk/dcmpstat/libsrc/dcmpstat.cc:88
4:16 in DcmPresentationState::createFromImage(DcmItem&, DVPSoverlayActivation, DVPSVOIActivation,
bool, bool, bool, DVPSGraphicLayering, char const*, char const*, char const*)
Shadow bytes around the buggy address:
```

```
  0x0000801313a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801313b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801313c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801313d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801313e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0000801313f0: 00 00 00 00 00 00 00 00 00[f9]f9 f9 f9 f9 f9
  0x000080131400: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x000080131410: 02 f9 f9 f9 f9 f9 f9 f9 04 f9 f9 f9 f9 f9 f9 f9
  0x000080131420: 00 00 f9 f9 f9 f9 f9 f9 00 00 05 f9 f9 f9 f9 f9
  0x000080131430: 00 05 f9 f9 f9 f9 f9 f9 02 f9 f9 f9 f9 f9 f9 f9
  0x000080131440: 04 f9 f9 f9 f9 f9 f9 f9 05 f9 f9 f9 f9 f9 f9 f9
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by karas:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==2532==ABORTING
```

This bug report was submitted on 2018-06-14 by GwanYeong Kim <gy741.kim@gmail.com>.

History

#1 - 2018-07-05 12:17 - Marco Eichelberg

- Category set to Library and Apps

- Status changed from New to Closed

- Assignee set to Marco Eichelberg

- % Done changed from 0 to 100

Closed by commit #6791085.

Files

POC_2018_06_14	1.24 KB	2018-06-15	Marco Eichelberg