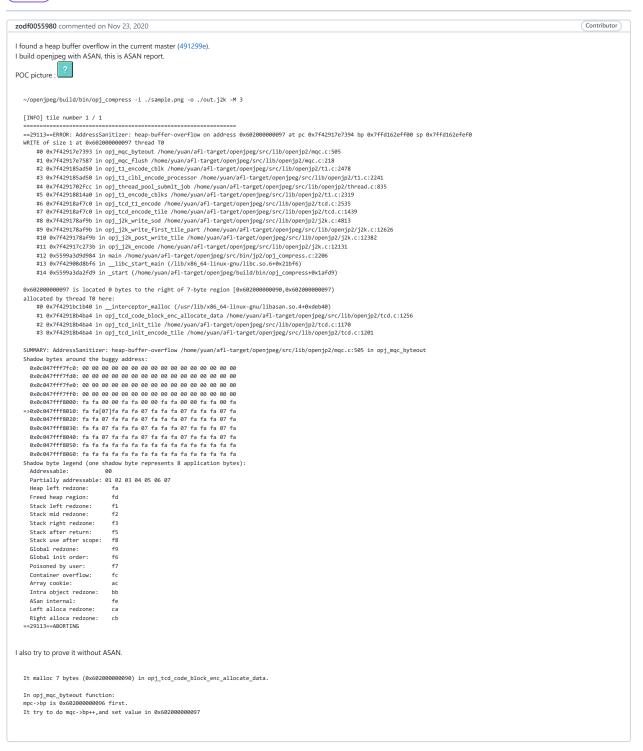
Jump to bottom

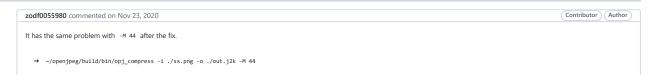
## Heap-buffer-overflow in lib/openjp2/mqc.c:499 #1283

New issue

○ Closed ) zodf0055980 opened this issue on Nov 23, 2020 · 4 comments



@ rouault closed this as completed in eaa@98b on Nov 23, 2020



```
[INFO] tile number 1 / 1
        ==13369==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000272f at pc 0x7f402686c0a0 bp 0x7fff404d6350 sp 0x7fff404d6340
       WRITE of size 1 at 0x60300000272f thread T0
               #0 0x7f402686c09f in opj_mqc_byteout /home/yuan/openjpeg/src/lib/openjp2/mqc.c:505
#1 0x7f402686c339 in opj_mqc_flush /home/yuan/openjpeg/src/lib/openjp2/mqc.c:218
              #2 0x7f40268e086f in opj_tl_encode_cblk /home/yuan/openjpeg/src/lib/openjp2/tl.c:2478
#3 0x7f40268e086f in opj_tl_cblk_encode_processor /home/yuan/openjpeg/src/lib/openjp2/tl.c:2241
#4 0x7f40267890ec in opj_thread_pool_submit_job /home/yuan/openjpeg/src/lib/openjp2/thread.c:835
               #5 0x7f40269074e4 in opj_t1_encode_cblks /home/yuan/openjpeg/src/lib/openjp2/tt.c:2319
#6 0x7f402693598e in opj_tcd_t1_encode /home/yuan/openjpeg/src/lib/openjp2/tcd.c:2537
               #7 0x7f402693598e in opj_tcd_encode_tile /home/yuan/openjpeg/src/lib/openjp2/tcd.c:1441
               #8 0x7f4026810b98 in opj j2k write sod /home/yuan/openjpeg/src/lib/openjp2/j2k.c:4813
               #9 0x7f4026810b98 in opj_j2k_write_first_tile_part /home/yuan/openjpeg/src/lib/openjp2/j2k.c:12626 #10 0x7f4026810b98 in opj_j2k_post_write_tile /home/yuan/openjpeg/src/lib/openjp2/j2k.c:12382
               #11 0x7f4026848236 in opj_j2k_encode /home/yuan/openjpeg/src/lib/openjp2/j2k.c:12131
#12 0x55cca6271705 in main /home/yuan/openjpeg/src/bin/jp2/opj_compress.c:2206
               #13 0x7f402595ebf6 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6) #14 0x55cca6276f19 in _start (/home/yuan/openjpeg/build/bin/opj_compress+0x1af19)
       0x6030000272f is located 0 bytes to the right of 31-byte region [0x603000002710,0x60300000272f) allocated by thread T0 here:
               #0 0x7f4026c46b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
#1 0x7f402693ab21 in opj_tcd_code_block_enc_allocate_data /home/yuan/openjpeg/src/lib/openjp2/tcd.c:1258
               #2 0x7f402693ab21 in opj_tcd_init_tile /home/yuan/openjpeg/src/lib/openjp2/tcd.c:1170
#3 0x7f402693ab21 in opj_tcd_init_encode_tile /home/yuan/openjpeg/src/lib/openjp2/tcd.c:1201
       SUMMARY: AddressSanitizer: heap-buffer-overflow /home/yuan/openjpeg/src/lib/openjp2/mqc.c:505 in opj_mqc_byteout
      Shadow bytes around the buggy address:

0xc067fff8490: 00 00 fa fa 00 00 00 fa fa 60 00 00 00 fa fa

0x0c067fff8400: 00 00 00 fa fa fa 60 00 00 00 fa fa

0x0c067fff8400: fa fa 60 00 00 00 fa fa 60 00 00 fa fa 60 00 00 fa
           0x0c067fff84c0: 00 00 fa fa 00 00 00 fa fa a 00 00 00 00 fa fa
         0x0c067fff84d0: 00 00 00 fa fa fa 00 00 00 00 fa fa 00 00 00 fa
=>0x0c067fff84e0: fa fa 00 00 00[07]fa fa 00 00 00 00 fa fa 00 00
           0x0c067fff84f0: 00 fa fa fa 00 00 00 fa fa 00 00 00 fa fa fa
           0x0c067fff8500: 00 00 00 07 fa fa 00 00 00 fa fa fa 00 00 00 fa 60 00 fa 60 00 00 fa 60 00 fa 60 00 00 fa 60 00 fa 60
           0x0c067fff8520: 00 07 fa fa 00 00 00 fa fa a 00 00 00 fa fa fa 60 0x0c067fff8530: 00 00 00 00 fa fa a 00 00 00 fa fa fa 60 0x0c067fff8530:
       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:
Stack left redzone:
            Stack mid redzone:
                                                             f2
           Stack right redzone:
Stack after return:
                                                             f5
           Stack use after scope:
Global redzone:
           Global init order:
           Poisoned by user:
            Container overflow:
                                                            fc
            Array cookie:
           Intra object redzone:
                                                            bb
            ASan internal:
          Left alloca redzone:
Right alloca redzone:
       ==13369==ABORTING
rouault added a commit that referenced this issue on Nov 23, 2020
          ⑤ Encoder: grow again buffer size in opj_tcd_code_block_enc_allocate_da... ...
                                                                                                                                                                                                                                                                                                                                                                     X 15cf3d9
  zodf0055980 commented on Nov 25, 2020 • edited -
                                                                                                                                                                                                                                                                                                                                        Contributor Author
   Submit PR #1285 avoid heap buffer overflow in -M 4 -IMF 2K
                                                                                                                                                                                                                                                                                                                                        Contributor Author
   zodf0055980 commented on Nov 28, 2020 • edited -
   This issue was assigned CVE-2020-27814.
   zodf0055980 commented on Dec 4, 2020
                                                                                                                                                                                                                                                                                                                                        Contributor Author
   find new POC ·
       ~/openjpeg/build/bin/opj_compress -i ./s0.png -o ./a.jp2 -n 8 -s 7,7 -M 4 -I
  Try to fix in #1303
DanielHeath pushed a commit to radiopaedia/openjpeg that referenced this issue on Sep 21, 2021
          Encoder: grow buffer size in opj_tcd_code_block_enc_allocate_data() t... ...
                                                                                                                                                                                                                                                                                                                                                                          ca9f403
DanielHeath pushed a commit to radiopaedia/openjpeg that referenced this issue on Sep 21, 2021
          Encoder: grow again buffer size in opj_tcd_code_block_enc_allocate_da... ...
DanielHeath pushed a commit to radiopaedia/openjpeg that referenced this issue on Sep 21, 2021
          Encoder: grow again buffer size in opj_tcd_code_block_enc_allocate_da... ...
                                                                                                                                                                                                                                                                                                                                                                          41fc486
```

Ç	DanielHeath pushed a commit to radiopaedia/openjpeg that referenced this issue on Sep 21, 2021	
	Encoder: grow again buffer size in opj_tcd_code_block_enc_allocate_da	fe959a3
乀	mtremer pushed a commit to ipfire/ipfire-2.x that referenced this issue on Apr 29	
	openjpeg: Update to version 2.4.0	ca98d29
Assign	nees	
No on	e assigned	
Labels		
None	yet	
Projec	ts	
None	yet	
Milest	one	
No mi	lestone	
Develo	opment	
No bra	anches or pull requests	
1 parti	cipant	