New issue

Jump to bottom

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

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

zodf0055980 commented on Nov 23, 2020 Contributor

I found a heap buffer overflow in the current master (491299e).
I build openjpeg with ASAN, this is ASAN report.

POC picture : 

```
~/openjpeg/build/bin/opj_compress -i ./sample.png -o ./out.j2k -M 3

[INFO] tile number 1 / 1
================================================================
==29113==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000097 at pc 0x7f42917e7394 bp 0x7ffd162eff00 sp 0x7ffd162efef0
WRITE of size 1 at 0x602000000097 thread T0
    #0 0x7f42917e7393 in opj_mqc_byteout /home/yuan/afl-target/openjpeg/src/lib/openjp2/mqc.c:505
    #1 0x7f42917e7587 in opj_mqc_flush /home/yuan/afl-target/openjpeg/src/lib/openjp2/mqc.c:218
    #2 0x7f429185ad50 in opj_t1_encode_cblk /home/yuan/afl-target/openjpeg/src/lib/openjp2/t1.c:2478
    #3 0x7f429185ad50 in opj_t1_clbl_encode_processor /home/yuan/afl-target/openjpeg/src/lib/openjp2/t1.c:2241
    #4 0x7f4291702fcc in opj_thread_pool_submit_job /home/yuan/afl-target/openjpeg/src/lib/openjp2/thread.c:835
    #5 0x7f42918814a0 in opj_t1_encode_cblks /home/yuan/afl-target/openjpeg/src/lib/openjp2/t1.c:2319
    #6 0x7f42918af7c0 in opj_tcd_t1_encode /home/yuan/afl-target/openjpeg/src/lib/openjp2/tcd.c:2535
    #7 0x7f42918af7c0 in opj_tcd_encode_tile /home/yuan/afl-target/openjpeg/src/lib/openjp2/tcd.c:1439
    #8 0x7f429178af9b in opj_j2k_write_sod /home/yuan/afl-target/openjpeg/src/lib/openjp2/j2k.c:4813
    #9 0x7f429178af9b in opj_j2k_write_first_tile_part /home/yuan/afl-target/openjpeg/src/lib/openjp2/j2k.c:12626
    #10 0x7f429178af9b in opj_j2k_post_write_tile /home/yuan/afl-target/openjpeg/src/lib/openjp2/j2k.c:12382
    #11 0x7f42917c273b in opj_j2k_encode /home/yuan/afl-target/openjpeg/src/lib/openjp2/j2k.c:12131
    #12 0x5599a3d9d984 in main /home/yuan/afl-target/openjpeg/src/bin/jp2/opj_compress.c:2206
    #13 0x7f42908d8bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #14 0x5599a3da2fd9 in _start (/home/yuan/afl-target/openjpeg/build/bin/opj_compress+0x1afd9)

0x602000000097 is located 0 bytes to the right of 7-byte region [0x602000000090,0x602000000097)
allocated by thread T0 here:
    #0 0x7f4291bc1b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f42918b4ba4 in opj_tcd_code_block_enc_allocate_data /home/yuan/afl-target/openjpeg/src/lib/openjp2/tcd.c:1256
    #2 0x7f42918b4ba4 in opj_tcd_init_tile /home/yuan/afl-target/openjpeg/src/lib/openjp2/tcd.c:1170
    #3 0x7f42918b4ba4 in opj_tcd_init_encode_tile /home/yuan/afl-target/openjpeg/src/lib/openjp2/tcd.c:1201

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/yuan/afl-target/openjpeg/src/lib/openjp2/mqc.c:505 in opj_mqc_byteout
Shadow bytes around the buggy address:
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 fa
=>0x0c047fff8010: fa fa[07]fa fa fa 07 fa fa fa 07 fa fa fa 07 fa
  0x0c047fff8020: fa fa 07 fa fa fa 07 fa fa fa 07 fa fa fa 07 fa
  0x0c047fff8030: fa fa 07 fa fa fa 07 fa fa fa 07 fa fa fa 07 fa
  0x0c047fff8040: fa fa 07 fa fa fa 07 fa fa fa 07 fa fa fa 07 fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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 user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==29113==ABORTING
```

I also try to prove it without ASAN.

```
It malloc 7 bytes (0x602000000090) in opj_tcd_code_block_enc_allocate_data.

In opj_mqc_byteout function:
mpc->bp is 0x602000000096 first.
It try to do mqc->bp++,and set value in 0x602000000097
```

rouault closed this as completed in eaa098b on Nov 23, 2020

zodf0055980 commented on Nov 23, 2020 Contributor Author

It has the same problem with `-M 44` after the fix.

```
→  ~/openjpeg/build/bin/opj_compress -i ./ss.png -o ./out.j2k -M 44
```

```
[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_t1_encode_cblk /home/yuan/openjpeg/src/lib/openjp2/t1.c:2478
    #3 0x7f40268e086f in opj_t1_cblk_encode_processor /home/yuan/openjpeg/src/lib/openjp2/t1.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/t1.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)

0x60300000272f 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:
  0x0c067fff8490: 00 00 fa fa 00 00 00 fa fa fa 00 00 00 00 fa fa
  0x0c067fff84a0: 00 00 00 fa fa fa 00 00 00 00 fa fa 00 00 00 fa
  0x0c067fff84b0: fa fa 00 00 00 00 00 fa fa 00 00 00 fa fa fa 00
  0x0c067fff84c0: 00 00 fa fa 00 00 00 fa fa fa 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 00 fa fa 00 00 00 fa fa fa
  0x0c067fff8500: 00 00 00 07 fa fa 00 00 00 00 fa fa 00 00 00 fa
  0x0c067fff8510: fa fa 00 00 00 00 fa fa 00 00 00 fa fa fa 00 00
  0x0c067fff8520: 00 07 fa fa 00 00 00 00 fa fa 00 00 00 fa fa fa
  0x0c067fff8530: 00 00 00 00 fa fa 00 00 00 fa fa fa 00 00 00 07
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 user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==13369==ABORTING
```

rouault added a commit that referenced this issue on Nov 23, 2020

`Encoder: grow again buffer size in opj_tcd_code_block_enc_allocate_da…` ··· ✕ `15cf3d9`

zodf0055980 commented on Nov 25, 2020 • edited — Contributor, Author

Submit PR #1285 avoid heap buffer overflow in `-M 4 -IMF 2K`

zodf0055980 commented on Nov 28, 2020 • edited — Contributor, Author

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…` ··· `c602f5e`

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`

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`

mtremer pushed a commit to ipfire/ipfire-2.x that referenced this issue on Apr 29

 `openjpeg: Update to version 2.4.0` ··· `ca98d29`

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant