Heap buffer overflow in libopenjp2 #1228

Closed **sebastianpoeplau** opened this issue on Jan 10, 2020 · 3 comments

sebastianpoeplau commented on Jan 10, 2020

Hi,

I found a heap buffer overflow that affects at least version 2.3.1 and current master (`ac37373`). On a regular build of openjpeg (in my case, the one shipped by Arch Linux), it leads to a crash; when building the project with address sanitizer, I get the following report:

```
$ bin/opj_decompress -i ../openjpeg_poc -o /tmp/image_verification.pgm

===========================================
The extension of this file is incorrect.
FOUND 1682. SHOULD BE .jp2
===========================================

[INFO] Start to read j2k main header (1277).
[INFO] Main header has been correctly decoded.
[INFO] No decoded area parameters, set the decoded area to the whole image
[INFO] Header of tile 1 / 33 has been read.
=================================================================
==31465==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000021c at pc 0x7fb82957229f bp 0x7ffe4b153d50 sp 0x7ffe4b153d48
WRITE of size 4 at 0x60700000021c thread T0
    #0 0x7fb82957229e in opj_t1_clbl_decode_processor (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x9f29e)
    #1 0x7fb8294e9a6c in opj_thread_pool_submit_job (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x16a6c)
    #2 0x7fb829566891 in opj_t1_decode_cblks (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x93891)
    #3 0x7fb8295b8790 in opj_tcd_decode_tile (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0xe5790)
    #4 0x7fb82951e632 in opj_j2k_decode_tile (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x4b632)
    #5 0x7fb829538e1e in opj_j2k_decode_tiles (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x65e1e)
    #6 0x7fb829524105 in opj_j2k_decode (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x51105)
    #7 0x7fb82954385b in opj_jp2_decode (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x7085b)
    #8 0x50e5d7 in main (/home/seba/tested_software/openjpeg_master/build_asan/bin/opj_decompress+0x50e5d7)
    #9 0x7fb82914d09a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2409a)
    #10 0x42f6f9 in _start (/home/seba/tested_software/openjpeg_master/build_asan/bin/opj_decompress+0x42f6f9)

0x60700000021c is located 0 bytes to the right of 60-byte region [0x6070000001e0,0x60700000021c)
allocated by thread T0 here:
    #0 0x4dbd79 in __interceptor_posix_memalign (/home/seba/tested_software/openjpeg_master/build_asan/bin/opj_decompress+0x4dbd79)
    #1 0x7fb8295c4f8f in opj_aligned_malloc (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0xf1f8f)
    #2 0x7fb8295b7b4a in opj_tcd_decode_tile (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0xe4b4a)
    #3 0x7fb82951e632 in opj_j2k_decode_tile (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x4b632)
    #4 0x7fb829538e1e in opj_j2k_decode_tiles (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x65e1e)
    #5 0x7fb829524105 in opj_j2k_decode (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x51105)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/seba/tested_software/openjpeg_master/build_asan/bin/libopenjp2.so.7+0x9f29e) in opj_t1_clbl_decode_processor
Shadow bytes around the buggy address:
  0x0c0e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c0e7fff8000: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c0e7fff8010: fa fa 00 00 00 00 00 00 00 00 00 00 fa fa fa fa
  0x0c0e7fff8020: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa 00 00
  0x0c0e7fff8030: 00 00 00 00 00 00 00 00 fa fa fa fa 00 00 00 00
=>0x0c0e7fff8040: 00 00 00[04]fa fa fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff8050: 00 04 fa fa fa fa fa fa 00 00 00 00 00 00 00 04
  0x0c0e7fff8060: fa fa fa fa fa fa fd fd fd fd fd fd fd fd fd fa
  0x0c0e7fff8070: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c0e7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8090: 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
  Shadow gap:              cc
==31465==ABORTING
```

For the report, I built with Clang 8.0.1 on Debian stable, using `CFLAGS=-fsanitize=address` and `CXXFLAGS=-fsanitize=address` , and calling CMake with `-DBUILD_THIRDPARTY=ON -DCMAKE_BUILD_TYPE=Release` .

The crashing input is available here. Since I believe this may be exploitable, I would like to request a CVE.

Let me know if I can help with more information. Thank you!

rouault added a commit to rouault/openjpeg that referenced this issue on Jan 10, 2020

`opj_j2k_update_image_dimensions(): reject images whose coordinates ar…` ··· d7064fa

rouault closed this as completed in `024b840` on Jan 11, 2020

rouault added a commit that referenced this issue on Jan 11, 2020

`Merge pull request #1229 from rouault/fix_1228` … `46c1eff`

sebastianpoeplau commented on Jan 11, 2020 Author

Great, thanks for the fast reaction!

sebastianpoeplau commented on Jan 13, 2020 Author

CVE 2020-6851 was assigned.

kloczek commented on Jan 18, 2020

Any chance to make quickly new release after commitong that fix?

sebastianpoeplau mentioned this issue on Jan 28, 2020

Another heap buffer overflow in libopenjp2 #1231

Closed

This was referenced on Mar 12, 2020

openjpeg: patch CVE-2020-6851 and CVE-2020-8112 NixOS/nixpkgs#82426

Merged

[20.03] openjpeg: patch CVE-2020-6851 and CVE-2020-8112 NixOS/nixpkgs#82444

Merged

[19.09] openjpeg: patch CVE-2020-6851 and CVE-2020-8112 NixOS/nixpkgs#82445

Merged

andreafioraldi added a commit to andreafioraldi/oss-fuzz that referenced this issue on Feb 17, 2021

`[openjpeg] Release cmake build type` … `6433d21`

andreafioraldi mentioned this issue on Feb 17, 2021

[openjpeg] Release cmake build type google/oss-fuzz#5209

Merged

inferno-chromium pushed a commit to google/oss-fuzz that referenced this issue on Feb 18, 2021

`[openjpeg] Release cmake build type (#5209)` … ✓ `f682792`

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

2 participants