New issue

Jump to bottom

Heap Use After Free in function gf_isom_dovi_config_get #2220

Closed 2 of 3 tasks **Janette88** opened this issue on Jul 5 · 1 comment

Janette88 commented on Jul 5 • edited

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

- [ ] I looked for a similar issue and couldn't find any.
- [x] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [x] I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...). I can share files anonymously with this dropbox: https://www.mediafire.com/filedrop/filedrop_hosted.php?drop=eec9e058a9486fe4e99c33021481d9e1826ca9dbc242a6cfaab0fe95da5e5d95

Detailed guidelines: http://gpac.io/2013/07/16/how-to-file-a-bug-properly/

Description

```
Heap use after free in fuction gf_isom_dovi_config_get located in isomedia/avc_ext.c:2490
```

System info

```
ubuntu 20.04 lts
```

version info:

```
 ./MP4Box -version
MP4Box - GPAC version 2.1-DEV-revUNKNOWN-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --enable-sanitizer
```

```
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SSL GPAC_HAS_SOCK_UN
GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D
```

compile

```
./configure --enable-sanitizer
make
```

crash command:

```
./MP4Box -info poc
```

poc :

poc.zip

Crash output:

```
[iso file] Unknown box type mp4u in parent stsd
[iso file] extra box maxr found in hinf, deleting
[iso file] extra box maxr found in hinf, deleting
[iso file] Unknown box type 80rak in parent moov
[iso file] Unknown box type drzf in parent dinf
[iso file] Missing dref box in dinf
[iso file] Incomplete box mdat - start 11495 size 853076
[iso file] Incomplete file while reading for dump - aborting parsing
# Movie Info - 5 tracks - TimeScale 90000
Duration 00:00:22.839 (recomputed 00:00:22.848)
Fragmented: no
Progressive (moov before mdat)
Major Brand isom - version 1 - compatible brands:
Created: GMT Wed Sep 14 06:08:31 2078
Modified: GMT Wed Sep 14 06:08:33 2078

File has root IOD (96 bytes)
Scene PL 0xff - Graphics PL 0xff - OD PL 0xff
Visual PL: Simple Profile @ Level 1 (0x01)
Audio PL: High Quality Audio Profile @ Level 2 (0x0f)
1 UDTA types:
        hnti:

# Track 1 Info - ID 1 - TimeScale 90000
Media Duration 00:00:22.800
Track flags: Enabled
Media Info: Language "Undetermined (und)" - Type "vide:mp4u" - 342 samples
Visual Sample Entry Info: width=176 height=144 (depth=24 bits)
Visual Track layout: x=0 y=0 width=176 height=144
=================================================================
==2234976==ERROR: AddressSanitizer: heap-use-after-free on address 0x60f000000130 at pc
0x7fbba822fbc0 bp 0x7ffe87b46740 sp 0x7ffe87b46730
READ of size 8 at 0x60f000000130 thread T0
    #0 0x7fbba822fbbf in gf_isom_dovi_config_get isomedia/avc_ext.c:2490
    #1 0x55f3db03107a in DumpTrackInfo /home/fuzz/gpac2.1/gpac/applications/mp4box/filedump.c:2862
```

```
    #2 0x55f3db03ea17 in DumpMovieInfo /home/fuzz/gpac2.1/gpac/applications/mp4box/filedump.c:3994
    #3 0x55f3db012ad0 in mp4box_main /home/fuzz/gpac2.1/gpac/applications/mp4box/mp4box.c:6367
    #4 0x7fbba58ed082 in __libc_start_main ../csu/libc-start.c:308
    #5 0x55f3dafe7afd in _start (/home/fuzz/gpac2.1/gpac/bin/gcc/MP4Box+0xa2afd)

0x60f000000130 is located 0 bytes inside of 168-byte region [0x60f000000130,0x60f0000001d8)
freed by thread T0 here:
    #0 0x7fbbab63440f in __interceptor_free
../../../../src/libsanitizer/asan/asan_malloc_linux.cc:122
    #1 0x7fbba825252d in unkn_box_read isomedia/box_code_base.c:793
    #2 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #3 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #4 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #5 0x7fbba82524fb in unkn_box_read isomedia/box_code_base.c:789
    #6 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #7 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #8 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #9 0x7fbba82524fb in unkn_box_read isomedia/box_code_base.c:789
    #10 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #11 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #12 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #13 0x7fbba82524fb in unkn_box_read isomedia/box_code_base.c:789
    #14 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #15 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #16 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #17 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #18 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #19 0x7fbba8302a35 in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #20 0x7fbba832babc in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:373
    #21 0x7fbba8331c2f in gf_isom_parse_movie_boxes isomedia/isom_intern.c:860
    #22 0x7fbba8331c2f in gf_isom_open_file isomedia/isom_intern.c:980
    #23 0x55f3db00c549 in mp4box_main /home/fuzz/gpac2.1/gpac/applications/mp4box/mp4box.c:6181
    #24 0x7fbba58ed082 in __libc_start_main ../csu/libc-start.c:308

previously allocated by thread T0 here:
    #0 0x7fbbab634808 in __interceptor_malloc
../../../../src/libsanitizer/asan/asan_malloc_linux.cc:144
    #1 0x7fbba82521ef in unkn_box_read isomedia/box_code_base.c:768
    #2 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #3 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #4 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #5 0x7fbba82524fb in unkn_box_read isomedia/box_code_base.c:789
    #6 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #7 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #8 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #9 0x7fbba82524fb in unkn_box_read isomedia/box_code_base.c:789
    #10 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #11 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #12 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #13 0x7fbba82524fb in unkn_box_read isomedia/box_code_base.c:789
    #14 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #15 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #16 0x7fbba830615a in gf_isom_box_array_read isomedia/box_funcs.c:1753
    #17 0x7fbba83015e3 in gf_isom_box_read isomedia/box_funcs.c:1860
    #18 0x7fbba83015e3 in gf_isom_box_parse_ex isomedia/box_funcs.c:271
    #19 0x7fbba8302a35 in gf_isom_parse_root_box isomedia/box_funcs.c:38
```

```
    #20 0x7fbba832babc in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:373
    #21 0x7fbba8331c2f in gf_isom_parse_movie_boxes isomedia/isom_intern.c:860
    #22 0x7fbba8331c2f in gf_isom_open_file isomedia/isom_intern.c:980
    #23 0x55f3db00c549 in mp4box_main /home/fuzz/gpac2.1/gpac/applications/mp4box/mp4box.c:6181
    #24 0x7fbba58ed082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-use-after-free isomedia/avc_ext.c:2490 in gf_isom_dovi_config_get
Shadow bytes around the buggy address:
  0x0c1e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1e7fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c1e7fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
=>0x0c1e7fff8020: fa fa fa fa fa fa[fd]fd fd fd fd fd fd fd fd fd
  0x0c1e7fff8030: fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa
  0x0c1e7fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8070: 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
==2234976==ABORTING
```

Impact

can cause a program to crash, use unexpected values, or execute code.

Occurrences:
avc_ext.c:2490

ps: this test was still based on the newest mp4box+asan. The bug happened in avc_ext.c:2490 which was the same location with the other issue i submitted (#2218). Maybe asan mistakenly reports "heap-use-after-free" instead of "heap-buffer-overflow". Pls check it again.

jeanlf commented on Jul 12 Contributor

fixed when fixing #2218, thanks for the poc

jeanlf closed this as completed on Jul 12

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants