New issue

Jump to bottom

# AddressSanitizer: heap-use-after-free in gf_isom_box_del isomedia/box_funcs.c:1696 #1661

Closed **Clingto** opened this issue on Dec 15, 2020 · 0 comments

**Clingto** commented on Dec 15, 2020 • edited

System info:
Ubuntu 16.04.6 LTS, X64, gcc 5.4.0, gpac (latest master `c4f8bc6` and the latest V1.0.1 `d8538e8` )

I think it is probably due to an imcomplete fix of #1340 、 #1440 and #1332.

Compile Command:

```
$ CC="gcc -fsanitize=address -g" CXX="g++ -fsanitize=address -g" ./configure --static-mp4box --extra-ldflags="-ldl -g"
$ make
```

Run Command:

```
$ MP4Box -hint $gf_isom_box_del-UAF -out /dev/null
```

POC file:
https://github.com/Clingto/POC/blob/master/gpac-MP4Box/gpac-c4f8bc6e_poc/gf_isom_box_del-UAF

gdb info:

```
Program received signal SIGSEGV, Segmentation fault.
__GI___libc_free (mem=0x7ffff6867010) at malloc.c:2958
2958    malloc.c: No such file or directory.
(gdb) bt
#0  __GI___libc_free (mem=0x7ffff6867010) at malloc.c:2958
#1  0x00000000008d8557 in co64_box_del ()
#2  0x0000000000053f9d4 in gf_isom_box_del ()
#3  0x0000000000053fa07 in gf_isom_box_del ()
#4  0x0000000000053fa07 in gf_isom_box_del ()
#5  0x0000000000053fa07 in gf_isom_box_del ()
#6  0x0000000000053fa07 in gf_isom_box_del ()
#7  0x0000000000053fa07 in gf_isom_box_del ()
#8  0x0000000000541407 in gf_isom_box_array_del ()
#9  0x0000000000054ab73 in gf_isom_delete_movie ()
#10 0x0000000000054d89d in gf_isom_close ()
#11 0x00000000004171c3 in mp4boxMain ()
#12 0x00007ffff6ec7840 in __libc_start_main (main=0x409dc0 <main>, argc=5, argv=0x7fffffffdf78, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fff
#13 0x00000000000409df9 in _start ()
```

ASAN info:

```
==17415==ERROR: AddressSanitizer: heap-use-after-free on address 0x60600000e7f8 at pc 0x000000736277 bp 0x7fff80125400 sp 0x7fff801253f0
READ of size 8 at 0x60600000e7f8 thread T0
    #0 0x736276 in gf_isom_box_del isomedia/box_funcs.c:1696
    #1 0x7361e6 in gf_isom_box_array_reset isomedia/box_funcs.c:346
    #2 0x7361e6 in gf_isom_box_array_del isomedia/box_funcs.c:352
    #3 0x7361e6 in gf_isom_box_del isomedia/box_funcs.c:1707
    #4 0x7361e6 in gf_isom_box_array_reset isomedia/box_funcs.c:346
    #5 0x7361e6 in gf_isom_box_array_del isomedia/box_funcs.c:352
    #6 0x7361e6 in gf_isom_box_del isomedia/box_funcs.c:1707
    #7 0x7361e6 in gf_isom_box_array_reset isomedia/box_funcs.c:346
    #8 0x7361e6 in gf_isom_box_array_del isomedia/box_funcs.c:352
    #9 0x7361e6 in gf_isom_box_del isomedia/box_funcs.c:1707
    #10 0x7361e6 in gf_isom_box_array_reset isomedia/box_funcs.c:346
    #11 0x7361e6 in gf_isom_box_array_del isomedia/box_funcs.c:352
    #12 0x7361e6 in gf_isom_box_del isomedia/box_funcs.c:1707
    #13 0x7361e6 in gf_isom_box_array_reset isomedia/box_funcs.c:346
    #14 0x7361e6 in gf_isom_box_array_del isomedia/box_funcs.c:352
    #15 0x7361e6 in gf_isom_box_del isomedia/box_funcs.c:1707
    #16 0x738e3e in gf_isom_box_array_reset isomedia/box_funcs.c:346
    #17 0x738e3e in gf_isom_box_array_del isomedia/box_funcs.c:352
    #18 0x7545bd in gf_isom_delete_movie isomedia/isom_intern.c:908
    #19 0x75bf4e in gf_isom_close isomedia/isom_read.c:618
    #20 0x42c0c0 in mp4boxMain /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:6718
    #21 0x7f6c5505883f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #22 0x417638 in _start (/opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/build/bin/MP4Box+0x417638)

0x60600000e7f8 is located 24 bytes inside of 56-byte region [0x60600000e7e0,0x60600000e818)
freed by thread T0 here:
    #0 0x7f6c560002ca in __interceptor_free (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x982ca)
    #1 0x7361af in gf_isom_box_del isomedia/box_funcs.c:1703
    #2 0x78000e in CleanWriters isomedia/isom_store.c:105
    #3 0x78000e in WriteInterleaved isomedia/isom_store.c:1728
    #4 0x7811f2 in WriteToFile isomedia/isom_store.c:1885
    #5 0x75ba6e in gf_isom_write isomedia/isom_read.c:592
    #6 0x75bf43 in gf_isom_close isomedia/isom_read.c:616
    #7 0x42c0c0 in mp4boxMain /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:6718
    #8 0x7f6c5505883f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

previously allocated by thread T0 here:
    #0 0x7f6c56000602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x102065d in co64_box_new isomedia/box_code_base.c:65
    #2 0x735fdf in gf_isom_box_new_ex isomedia/box_funcs.c:1582
```

```
    #3 0x735fdf in gf_isom_box_new isomedia/box_funcs.c:1605
    #4 0x7feec4 in stbl_AddOffset isomedia/stbl_write.c:1989
    #5 0x7feec4 in stbl_SetChunkAndOffset isomedia/stbl_write.c:2090
    #6 0x77f65a in DoInterleave isomedia/isom_store.c:1537
    #7 0x780197 in WriteInterleaved isomedia/isom_store.c:1665
    #8 0x7811f2 in WriteToFile isomedia/isom_store.c:1885
    #9 0x75ba6e in gf_isom_write isomedia/isom_read.c:592
    #10 0x75bf43 in gf_isom_close isomedia/isom_read.c:616
    #11 0x42c0c0 in mp4boxMain /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:6718
    #12 0x7f6c5505883f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

SUMMARY: AddressSanitizer: heap-use-after-free isomedia/box_funcs.c:1696 gf_isom_box_del
Shadow bytes around the buggy address:
  0x0c0c7fff9ca0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff9cb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff9cc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff9cd0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0c7fff9ce0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c0c7fff9cf0: fa fa fa fa fa fa fa fa fa fa fa fa fd fd fd[fd]
  0x0c0c7fff9d00: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fa
  0x0c0c7fff9d10: fa fa fa fa 00 00 00 00 00 00 00 00 fa fa fa fa
  0x0c0c7fff9d20: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c0c7fff9d30: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c7fff9d40: fa fa fa fa fd fd fd fd fd fd fd fd 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==17415==ABORTING
```

Addition: This bug was found with our fuzzer, which is based on AFL. Our fuzzer is developed by Yuanpingyu(cfenicey@gmail.com) 、Xiangkun Jia(xiangkun@iscas.ac.cn) 、Marsman1996(lqliuyuwei@outlook.com) and Yanhao.

**jeanlf** closed this as completed in 5aba276 on Jan 4, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant