gpac / **gpac** Public

Code · **Issues** 11 · Pull requests 2 · Wiki · Security · Insights

New issue

Jump to bottom

# There is a heap buffer overflow detected by AddressSanitizer #2120

Closed **AAArdu** opened this issue on Feb 16 · 0 comments

**AAArdu** commented on Feb 16

## Description

There is a heap buffer overflow detected by AddressSanitizer

## System info

```
Ubuntu 20.04.2 LTS
clang version 12.0.0-++20210402082642+04ba60cfe598-1~exp1~20210402063359.71
MP4Box - GPAC version 1.1.0-DEV-rev1759-geb2d1e6dd-master
```

## Build command

```
./configure --static-mp4box --prefix=`realpath ./install` --enable-sanitizer --cc=clang --
cxx=clang++
```

## crash command

```
MP4Box -frag 1 -out /dev/null poc_file
```

## Pocs

poc.zip

## Crash output

```
==36294==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000014f5 at pc
0x0000007ed95d bp 0x7fff9dbe5110 sp 0x7fff9dbe5108
READ of size 1 at 0x6020000014f5 thread T0
    #0 0x7ed95c in gf_isom_apple_enum_tag
/programs/mp4box/builds/build15/src/isomedia/isom_read.c:4347:9
    #1 0x1578ec6 in isor_declare_track
/programs/mp4box/builds/build15/src/filters/isoffin_load.c:787:8
    #2 0x1583b47 in isor_declare_objects
/programs/mp4box/builds/build15/src/filters/isoffin_load.c:1453:3
    #3 0xd05c0d in isoffin_initialize
/programs/mp4box/builds/build15/src/filters/isoffin_read.c:485:8
    #4 0xb74a43 in gf_filter_new_finalize
/programs/mp4box/builds/build15/src/filter_core/filter.c:441:8
    #5 0xb73120 in gf_filter_new /programs/mp4box/builds/build15/src/filter_core/filter.c:395:7
    #6 0xb5e1bb in gf_fs_load_filter_internal
/programs/mp4box/builds/build15/src/filter_core/filter_session.c:1293:13
    #7 0x911528 in gf_media_fragment_file
/programs/mp4box/builds/build15/src/media_tools/isom_tools.c:3789:6
    #8 0x4e6fdc in mp4boxMain /programs/mp4box/builds/build15/applications/mp4box/main.c:6439:7
    #9 0x7f7b5af220b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #10 0x41ea6d in _start (/programs/mp4box/builds/build15/bin/gcc/MP4Box+0x41ea6d)

0x6020000014f5 is located 0 bytes to the right of 5-byte region [0x6020000014f0,0x6020000014f5)
allocated by thread T0 here:
    #0 0x499ccd in malloc (/programs/mp4box/builds/build15/bin/gcc/MP4Box+0x499ccd)
    #1 0x12c648d in databox_box_read
/programs/mp4box/builds/build15/src/isomedia/box_code_apple.c:247:22
    #2 0x7ae1ed in gf_isom_box_read
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1826:9
    #3 0x7ae1ed in gf_isom_box_parse_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:264:14
    #4 0x12c53c3 in ilst_item_box_read
/programs/mp4box/builds/build15/src/isomedia/box_code_apple.c:114:7
    #5 0x7ae1ed in gf_isom_box_read
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1826:9
    #6 0x7ae1ed in gf_isom_box_parse_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:264:14
    #7 0x12c4d35 in ilst_box_read
/programs/mp4box/builds/build15/src/isomedia/box_code_apple.c:47:8
    #8 0x7ae1ed in gf_isom_box_read
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1826:9
    #9 0x7ae1ed in gf_isom_box_parse_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:264:14
    #10 0x7affe3 in gf_isom_box_array_read_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1719:7
    #11 0x132290a in meta_box_read
/programs/mp4box/builds/build15/src/isomedia/box_code_meta.c:106:13
    #12 0x7ae1ed in gf_isom_box_read
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1826:9
    #13 0x7ae1ed in gf_isom_box_parse_ex
```

```
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:264:14
    #14 0x7affe3 in gf_isom_box_array_read_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1719:7
    #15 0x12f6245 in udta_box_read
/programs/mp4box/builds/build15/src/isomedia/box_code_base.c:8075:13
    #16 0x7ae1ed in gf_isom_box_read
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1826:9
    #17 0x7ae1ed in gf_isom_box_parse_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:264:14
    #18 0x7affe3 in gf_isom_box_array_read_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1719:7
    #19 0x7ae1ed in gf_isom_box_read
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:1826:9
    #20 0x7ae1ed in gf_isom_box_parse_ex
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:264:14
    #21 0x7ad3c1 in gf_isom_parse_root_box
/programs/mp4box/builds/build15/src/isomedia/box_funcs.c:38:8
    #22 0x7c8dc1 in gf_isom_parse_movie_boxes_internal
/programs/mp4box/builds/build15/src/isomedia/isom_intern.c:351:7
    #23 0x7c8dc1 in gf_isom_parse_movie_boxes
/programs/mp4box/builds/build15/src/isomedia/isom_intern.c:814:6
    #24 0x7cd1a6 in gf_isom_open_file
/programs/mp4box/builds/build15/src/isomedia/isom_intern.c:934:19
    #25 0x4e14d6 in mp4boxMain /programs/mp4box/builds/build15/applications/mp4box/main.c:5968:12
    #26 0x7f7b5af220b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow
/programs/mp4box/builds/build15/src/isomedia/isom_read.c:4347:9 in gf_isom_apple_enum_tag
Shadow bytes around the buggy address:
  0x0c047fff8240: fa fa fd fd fa fa fd fd fa fa fd fa fa fa 00 00
  0x0c047fff8250: fa fa 00 00 fa fa 00 00 fa fa 00 04 fa fa 00 fa
  0x0c047fff8260: fa fa 00 00 fa fa 00 00 fa fa 01 fa fa fa 00 00
  0x0c047fff8270: fa fa 00 05 fa fa 00 00 fa fa 00 01 fa fa 00 00
  0x0c047fff8280: fa fa 00 00 fa fa 02 fa fa fa 00 00 fa fa 00 02
=>0x0c047fff8290: fa fa 00 00 fa fa 00 04 fa fa 00 00 fa fa[05]fa
  0x0c047fff82a0: fa fa 00 00 fa fa 02 fa fa fa 00 00 fa fa 00 fa
  0x0c047fff82b0: fa fa 00 00 fa fa 00 00 fa fa 06 fa fa fa 00 00
  0x0c047fff82c0: fa fa 02 fa fa fa 00 00 fa fa 02 fa fa fa 00 00
  0x0c047fff82d0: fa fa 03 fa fa fa 00 00 fa fa 02 fa fa fa 00 00
  0x0c047fff82e0: fa fa 00 00 fa fa 00 03 fa fa 00 00 fa fa 00 00
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
==36294==ABORTING
```

**jeanlf** closed this as completed in `f0a41d1` on Feb 16

**Assignees**

No one assigned

**Labels**

None yet

**Projects**

None yet

**Milestone**

No milestone

**Development**

No branches or pull requests

**1 participant**