New issue

Jump to bottom

heap-buffer-overflow in MP4BOX at souce file src/isomedia/hint_track.c:46 #1894

Closed 3 tasks done **AntsKnows** opened this issue on Aug 26, 2021 · 0 comments

AntsKnows commented on Aug 26, 2021 • edited

- [x] 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 ...).

It's a heap-buffer-overflow bug

Step to reproduce:
1.get latest commit code (GPAC version 1.1.0-DEV-rev1170-g592ba26-master)
2.compile with --enable-sanitizer
3.run ./MP4BOX info poc

Env:
Ubunut 20.04 , clang 12.0.1

ASAN report

```
==2275020==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x604000000638 at pc 0x7f1c17ca68a4 bp 0x7ffd52eab1d0 sp 0x7ffd52eab1c8
READ of size 4 at 0x604000000638 thread T0
    #0 0x7f1c17ca68a3 in GetHintFormat /home/lly/pro/gpac_public/src/isomedia/hint_track.c:46:22
    #1 0x7f1c17ca68a3 in CheckHintFormat /home/lly/pro/gpac_public/src/isomedia/hint_track.c:58:6
    #2 0x7f1c17ca68a3 in gf_isom_get_payt_count /home/lly/pro/gpac_public/src/isomedia/hint_track.c:979:7
    #3 0x5b52e5 in DumpTrackInfo /home/lly/pro/gpac_public/applications/mp4box/filedump.c:3178:14
    #4 0x5e4af1 in DumpMovieInfo /home/lly/pro/gpac_public/applications/mp4box/filedump.c:3789:3
    #5 0x52ea16 in mp4boxMain /home/lly/pro/gpac_public/applications/mp4box/main.c:6023:9
    #6 0x7f1c15d710b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
    #7 0x429aad in _start (/home/lly/pro/gpac_public/bin/gcc/MP4Box+0x429aad)

0x604000000638 is located 0 bytes to the right of 40-byte region [0x604000000610,0x604000000638)
allocated by thread T0 here:
    #0 0x4a496d in malloc (/home/lly/pro/gpac_public/bin/gcc/MP4Box+0x4a496d)
    #1 0x7f1c17543a17 in nmhd_box_new /home/lly/pro/gpac_public/src/isomedia/box_code_base.c:4651:2
    #2 0x7f1c1775de4f in gf_isom_box_new_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1673:6
    #3 0x7f1c17756209 in gf_isom_box_parse_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:239:12
    #4 0x7f1c17760a0b in gf_isom_box_array_read_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1707:7
    #5 0x7f1c1751e43a in minf_box_read /home/lly/pro/gpac_public/src/isomedia/box_code_base.c:3527:6
    #6 0x7f1c17757fe8 in gf_isom_box_read /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1810:9
    #7 0x7f1c17757fe8 in gf_isom_box_parse_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:263:14
    #8 0x7f1c17760a0b in gf_isom_box_array_read_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1707:7
    #9 0x7f1c17511b3d in mdia_box_read /home/lly/pro/gpac_public/src/isomedia/box_code_base.c:3078:6
    #10 0x7f1c17757fe8 in gf_isom_box_read /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1810:9
    #11 0x7f1c17757fe8 in gf_isom_box_parse_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:263:14
    #12 0x7f1c17760a0b in gf_isom_box_array_read_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1707:7
    #13 0x7f1c17582c10 in trak_box_read /home/lly/pro/gpac_public/src/isomedia/box_code_base.c:6734:6
    #14 0x7f1c17757fe8 in gf_isom_box_read /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1810:9
    #15 0x7f1c17757fe8 in gf_isom_box_parse_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:263:14
    #16 0x7f1c17760a0b in gf_isom_box_array_read_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1707:7
    #17 0x7f1c17757fe8 in gf_isom_box_read /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:1810:9
    #18 0x7f1c17757fe8 in gf_isom_box_parse_ex /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:263:14
    #19 0x7f1c177548b9 in gf_isom_parse_root_box /home/lly/pro/gpac_public/src/isomedia/box_funcs.c:38:8
    #20 0x7f1c177e2347 in gf_isom_parse_movie_boxes_internal /home/lly/pro/gpac_public/src/isomedia/isom_intern.c:320:7
    #21 0x7f1c177e2347 in gf_isom_parse_movie_boxes /home/lly/pro/gpac_public/src/isomedia/isom_intern.c:781:6
    #22 0x7f1c177f84d3 in gf_isom_open_file /home/lly/pro/gpac_public/src/isomedia/isom_intern.c:901:19
    #23 0x53c4b8 in mp4boxMain /home/lly/pro/gpac_public/applications/mp4box/main.c:5841:12
    #24 0x7f1c15d710b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/lly/pro/gpac_public/src/isomedia/hint_track.c:46:22 in GetHintFormat
Shadow bytes around the buggy address:
  0x0c087fff8070: fa fa 00 00 00 00 04 fa fa fa 00 00 00 00 00 00
  0x0c087fff8080: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c087fff8090: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
  0x0c087fff80a0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
  0x0c087fff80b0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
=>0x0c087fff80c0: fa fa 00 00 00 00 00[fa]fa fa 00 00 00 00 00 00
  0x0c087fff80d0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
  0x0c087fff80e0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff80f0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
  0x0c087fff8100: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 00
  0x0c087fff8110: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 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
```

poc.zip

jeanlf closed this as completed in 86c1566 on Aug 30, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant