New issue

Jump to bottom

[Security]heap-buffer-overflow in abst_box_read #1733

Closed **5n1p3r0010** opened this issue on Apr 8, 2021 · 0 comments

5n1p3r0010 commented on Apr 8, 2021

Hi,

There is a heap buffer overflow issue with gpac MP4Box,this can reproduce on the lattest commit.

Steps To Reproduce

build:

```
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" LDFLAGS="-fsanitize=address" ./configure
make
```

run as:

```
MP4Box -hint <poc> -out /dev/null
```

shows the following log:

```
==807129==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000101f at pc 0x7fed7a3e739d bp 0x7ffef6967980 sp 0x7ffef6967128
READ of size 16 at 0x60200000101f thread T0
    #0 0x7fed7a3e739c in strdup (/lib/x86_64-linux-gnu/libasan.so.5+0x9639c)
    #1 0x7fed79a39ac1 in gf_strdup utils/alloc.c:170
    #2 0x7fed79ca1e53 in abst_box_read isomedia/box_code_adobe.c:110
    #3 0x7fed79c36b9d in gf_isom_box_read isomedia/box_funcs.c:1801
    #4 0x7fed79c3543f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #5 0x7fed79c34938 in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #6 0x7fed79c3f101 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:318
    #7 0x7fed79c40855 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:750
    #8 0x7fed79c40be8 in gf_isom_open_file isomedia/isom_intern.c:870
    #9 0x7fed79c43bc4 in gf_isom_open isomedia/isom_read.c:520
    #10 0x55a900236d8a in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5699
    #11 0x55a90023954d in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #12 0x7fed797c00b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #13 0x55a90022520d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1820d)

0x60200000101f is located 0 bytes to the right of 15-byte region [0x602000001010,0x60200000101f)
allocated by thread T0 here:
    #0 0x7fed7a45ebc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7fed79a39a32 in gf_malloc utils/alloc.c:150
    #2 0x7fed79ca1d3f in abst_box_read isomedia/box_code_adobe.c:97
    #3 0x7fed79c36b9d in gf_isom_box_read isomedia/box_funcs.c:1801
    #4 0x7fed79c3543f in gf_isom_box_parse_ex isomedia/box_funcs.c:260
    #5 0x7fed79c34938 in gf_isom_parse_root_box isomedia/box_funcs.c:38
    #6 0x7fed79c3f101 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:318
    #7 0x7fed79c40855 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:750
    #8 0x7fed79c40be8 in gf_isom_open_file isomedia/isom_intern.c:870
    #9 0x7fed79c43bc4 in gf_isom_open isomedia/isom_read.c:520
    #10 0x55a900236d8a in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5699
    #11 0x55a90023954d in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #12 0x7fed797c00b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/lib/x86_64-linux-gnu/libasan.so.5+0x9639c) in strdup
Shadow bytes around the buggy address:
  0x0c047fff81b0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff81c0: fa fa 00 07 fa fa 07 fa fa fa fd fa fa fa 04 fa
  0x0c047fff81d0: fa fa 00 02 fa fa fd fa fa fa 00 07 fa fa 00 00
  0x0c047fff81e0: fa fa 00 00 fa fa 00 fa fa fa fd fa fa fa 00 00
  0x0c047fff81f0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff8200: fa fa 00[07]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8210: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8230: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8240: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8250: 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
==807129==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
heap-buffer-overflow.zip

jeanlf closed this as completed in 758135e on Apr 8, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant