New issue

Jump to bottom

[Security]heap buffer overflow issue with gpac MP4Box #1703

Closed **5n1p3r0010** opened this issue on Mar 11, 2021 · 0 comments

5n1p3r0010 commented on Mar 11, 2021 • edited

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:

```
=================================================================
==114880==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x607000000a80 at pc 0x7f469397c57d bp 0x7fffe55ec240 sp 0x7fffe55eb9e8
WRITE of size 138 at 0x607000000a80 thread T0
    #0 0x7f469397c57c  (/lib/x86_64-linux-gnu/libasan.so.5+0x9b57c)
    #1 0x7f4693177812 in gf_bs_read_data (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0xa6812)
    #2 0x7f46932d4ffa in tenc_box_read (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x203ffa)
    #3 0x7f46932ebc68 in gf_isom_box_parse_ex (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x21ac68)
    #4 0x7f46932ec33f in gf_isom_parse_root_box (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x21b33f)
    #5 0x7f46932f3fd9 in gf_isom_parse_movie_boxes_internal (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x222fd9)
    #6 0x7f46932f55a8 in gf_isom_open_file (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x2245a8)
    #7 0x55cb0df407ad in mp4boxMain (/home/r00t/fuzz/target/gpac/bin/gcc/MP4Box+0x287ad)
    #8 0x7f4692f060b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #9 0x55cb0df3026d in _start (/home/r00t/fuzz/target/gpac/bin/gcc/MP4Box+0x1826d)

0x607000000a80 is located 0 bytes to the right of 80-byte region [0x607000000a30,0x607000000a80)
allocated by thread T0 here:
    #0 0x7f46939eebc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f46932d4ec1 in tenc_box_new (/home/r00t/fuzz/target/gpac/bin/gcc/libgpac.so.10+0x203ec1)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/lib/x86_64-linux-gnu/libasan.so.5+0x9b57c)
Shadow bytes around the buggy address:
  0x0c0e7fff8100: 00 00 00 00 00 00 00 00 00 02 fa fa fa fa 00 00
  0x0c0e7fff8110: 00 00 00 00 00 00 06 fa fa fa fa fa 00 00 00 00
  0x0c0e7fff8120: 00 00 00 00 00 00 fa fa fa fa 00 00 00 00 00 00
  0x0c0e7fff8130: 00 00 00 00 fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff8140: 00 00 fa fa fa fa 00 00 00 00 00 00 00 00 00 00
=>0x0c0e7fff8150:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8170: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81a0: 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
==114880==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab

gpac-heap_overflow1.zip

jeanlf closed this as completed in 8986422 on Mar 11, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant