New issue

Jump to bottom

heap buffer overflow issue with gpac MP4Box #1840

Closed **dhbbb** opened this issue on Jul 5, 2021 · 0 comments

dhbbb commented on Jul 5, 2021

Hello,
A heap-buffer-overflow has occurred when running program MP4Box,which leads to a Deny of Service caused by dividing zero without sanity check,this can reproduce on the lattest commit.
System info：
Ubuntu 20.04.1 : clang 10.0.0 , gcc 9.3.0

poc.zip

file: media.c
function:gf_isom_get_3gpp_audio_esd
line: 105
As below code shows:

```
97              gf_bs_write_data(bs, "\x41\x6D\x7F\x5E\x15\xB1\xD0\x11\xBA\x91\x00\x80\x5F\xB4\xB9\x7E", 16);
98              gf_bs_write_u16_le(bs, 1);
99              memset(szName, 0, 80);
100             strcpy(szName, "QCELP-13K(GPAC-emulated)");
101             gf_bs_write_data(bs, szName, 80);
102             ent = &stbl->TimeToSample->entries[0];
103             sample_rate = entry->samplerate_hi;
104             block_size = ent ? ent->sampleDelta : 160;
105             gf_bs_write_u16_le(bs, 8*sample_size*sample_rate/block_size);      <------ block_size can be zero
106             gf_bs_write_u16_le(bs, sample_size);
107             gf_bs_write_u16_le(bs, block_size);
108             gf_bs_write_u16_le(bs, sample_rate);
109             gf_bs_write_u16_le(bs, entry->bitspersample);
110             gf_bs_write_u32_le(bs, sample_size ? 0 : 7);
```

Verification steps：
1.Get the source code of gpac
2.Compile

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

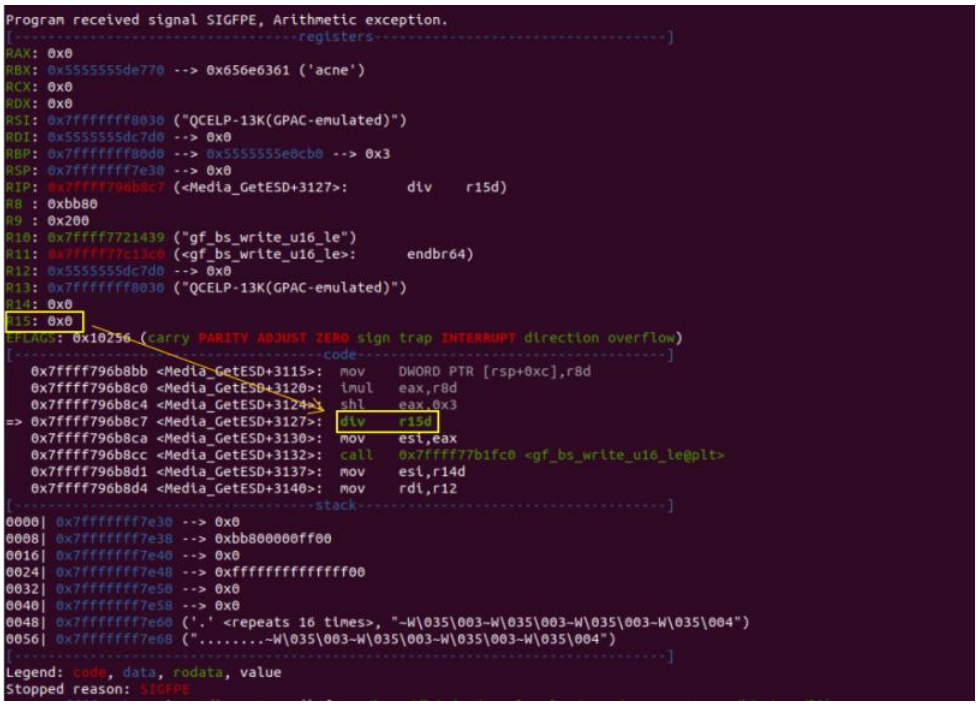
3.run MP4Box

```
./MP4Box -hint poc -out /dev/null
```

In Command line:

```
[iso file] Unknown box type esJs in parent enca
[iso file] Unknown box type stts in parent enca
[iso file] Box "enca" (start 1455) has 5 extra bytes
[iso file] Box "enca" is larger than container box
[iso file] Box "stsd" size 171 (start 1439) invalid (read 192)
Floating point exception
```

gdb info



asan info

```
=================================================================
==967870==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001874 at pc 0x7f3a53c0836c bp 0x7ffcce36e790 sp 0x7ffcce36e780
READ of size 4 at 0x602000001874 thread T0
    #0 0x7f3a53c0836b in gf_isom_get_3gpp_audio_esd isomedia/media.c:104
    #1 0x7f3a53c0836b in Media_GetESD isomedia/media.c:330
    #2 0x7f3a53b1ac04 in gf_isom_get_decoder_config isomedia/isom_read.c:1329
    #3 0x7f3a53b56d2e in gf_isom_guess_specification isomedia/isom_read.c:4035
    #4 0x5602827ad1d1 in HintFile /home/.../gpac/gpac-master-A/applications/mp4box/main.c:3379
    #5 0x5602827c4d54 in mp4boxMain /home/.../gpac/gpac-master-A/applications/mp4box/main.c:6297
    #6 0x7f3a52d080b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #7 0x560282777f1d in _start (/home/.../gpac/gpac-master-A/bin/gcc/MP4Box+0x48f1d)

0x602000001874 is located 3 bytes to the right of 1-byte region [0x602000001870,0x602000001871)
allocated by thread T0 here:
    #0 0x7f3a55be6bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f3a539e10ec in stts_box_read isomedia/box_code_base.c:5788

SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/media.c:104 in gf_isom_get_3gpp_audio_esd
Shadow bytes around the buggy address:
  0x0c047fff82b0: fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff82c0: fa fa fd fd fa fa fd fd fa fa fd fa fa fa 00 00
  0x0c047fff82d0: fa fa 01 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff82e0: fa fa 00 00 fa fa 01 fa fa fa 00 00 fa fa 00 00
  0x0c047fff82f0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff8300: fa fa 00 00 fa fa 00 fa fa fa 00 00 fa fa[01]fa
  0x0c047fff8310: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 fa
  0x0c047fff8320: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8330: fa fa 01 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8340: fa fa 00 00 fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8350: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
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
==967870==ABORTING
```

jeanlf closed this as completed in 6007c71 on Jul 5, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant