New issue

Jump to bottom

# A heap-buffer-overflow has occurred in function gf_isom_dovi_config_get #1846

Closed **dhbbb** opened this issue on Jul 6, 2021 · 0 comments

**dhbbb** commented on Jul 6, 2021

Hello,
A heap-buffer-overflow has occurred in function gf_isom_dovi_config_get of isomedia/avc_ext.c:2435 when running program MP4Box,this can reproduce on the lattest commit.
System info：
Ubuntu 20.04.1 : clang 10.0.0 , gcc 9.3.0

poc_heap.zip

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 -info poc.mp4
```

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)
* Movie Info *
        Timescale 90000 - 2 tracks
Segmentation fault
```

asan info

```
=================================================================
==1042542==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x610000000130 at pc 0x7fc6ede92514 bp 0x7ffcfced6850 sp 0x7ffcfced6840
READ of size 8 at 0x610000000130 thread T0
    #0 0x7fc6ede92513 in gf_isom_dovi_config_get isomedia/avc_ext.c:2435
    #1 0x7fc6ee2fec1e in gf_media_get_rfc_6381_codec_name media_tools/isom_tools.c:4207
    #2 0x558b1bf03ac5 in DumpTrackInfo /home.../gpac/gpac-master/applications/mp4box/filedump.c:3442
    #3 0x558b1bf18f44 in DumpMovieInfo /home.../gpac/gpac-master/applications/mp4box/filedump.c:3777
    #4 0x558b1bed571d in mp4boxMain /home.../gpac/gpac-master/applications/mp4box/main.c:5991
    #5 0x7fc6ed2390b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #6 0x558b1be77f1d in _start (/home.../gpac/gpac-master/bin/gcc/MP4Boxfl+0x48f1d)

Address 0x610000000130 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/avc_ext.c:2435 in gf_isom_dovi_config_get
Shadow bytes around the buggy address:
  0x0c207fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c207fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c207fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c207fff8020: fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa
  0x0c207fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c207fff8070: 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
==1042542==ABORTING
```

source code

```
2428 GF_DOVIDecoderConfigurationRecord *gf_isom_dovi_config_get(GF_ISOFile* the_file, u32 trackNumber, u32 DescriptionIndex)
2429 {
```

```
2430    GF_TrackBox* trak;
2431    GF_MPEGVisualSampleEntryBox *entry;
2432    trak = gf_isom_get_track_from_file(the_file, trackNumber);
2433    if (!trak || !trak->Media || !DescriptionIndex) return NULL;
2434    entry = (GF_MPEGVisualSampleEntryBox*)gf_list_get(trak->Media->information->sampleTable->SampleDescription->child_boxes, DescriptionIndex - 1);
2435    if (!entry || !entry->dovi_config) return NULL;
2436    return DOVI_DuplicateConfig(&entry->dovi_config->DOVIConfig);
2437 }
```

**jeanlf** closed this as completed in `737e1f3` on Jul 7, 2021

**Janette88** mentioned this issue on Jul 6

**heap-buffer-overflow in function gf_isom_dovi_config_get** #2218

Closed

3 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant