gpac / gpac Public

Code Issues 9 Pull requests 2 Wiki Security Insights

New issue Jump to bottom

heap-buffer-overflow in function gf_isom_dovi_config_get #2218

Closed 2 of 3 tasks Janette88 opened this issue on Jul 4 · 0 comments

Janette88 commented on Jul 4 • edited

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

- □ I looked for a similar issue and couldn't find any.
- ☑ I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- ☑ I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...). I can share files anonymously with this dropbox: https://www.mediafire.com/filedrop/filedrop_hosted.php?drop=eec9e058a9486fe4e99c33021481d9e1826ca9dbc242a6cfaab0fe95da5e5d95

Detailed guidelines: http://gpac.io/2013/07/16/how-to-file-a-bug-properly/

Description

A heap-buffer-overflow has occurred in function gf_isom_dovi_config_get of isomedia/avc_ext.c:2490 when running program MP4Box,this can reproduce on the lattest commit.

version info

```
fuzz@ubuntu:~/gpac2.1/gpac/bin/gcc$ ./MP4Box -version
MP4Box - GPAC version 2.1-DEV-revUNKNOWN-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --enable-sanitizer
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SSL GPAC_HAS_SOCK_UN
GPAC_MINIMAL_ODF GPAC_HAS_QJS GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D
```

crash command

```
./MP4Box -info poc1
```

crash output

```

[iso file] Unknown box type 00000200 in parent stsd
# Movie Info - 1 track - TimeScale 1000
Duration 00:00:10.000 (recomputed 4 Days, 14:43:47.879)
Fragmented: no
Major Brand mp4@ - version 0 - compatible brands: mp42 mp41 isom iso2
Created: GMT Thu Apr 26 09:02:13 2012


# Track 1 Info - ID 1 - TimeScale 3000
Media Duration 00:00:10.000  (recomputed 4 Days, 14:43:47.879)
Track flags: Enabled In Movie In Preview
Media Info: Language "Undetermined (und)" - Type "vide:00000200" - 300 samples
Visual Sample Entry Info: width=320 height=240 (depth=24 bits)
Visual Track layout: x=0 y=0 width=320 height=240
=================================================================
==2235126==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60f000000130 at pc
0x7ff2a69b3bc0 bp 0x7fff43da89f0 sp 0x7fff43da89e0
READ of size 8 at 0x60f000000130 thread T0
    #0 0x7ff2a69b3bbf in gf_isom_dovi_config_get isomedia/avc_ext.c:2490
    #1 0x56165102107a in DumpTrackInfo /home/fuzz/gpac2.1/gpac/applications/mp4box/filedump.c:2862
    #2 0x56165102ea17 in DumpMovieInfo /home/fuzz/gpac2.1/gpac/applications/mp4box/filedump.c:3994
    #3 0x561651002ad0 in mp4box_main /home/fuzz/gpac2.1/gpac/applications/mp4box/mp4box.c:6367
    #4 0x7ff2a4071082 in __libc_start_main ../csu/libc-start.c:308
    #5 0x561650fd7afd in _start (/home/fuzz/gpac2.1/gpac/bin/gcc/MP4Box+0xa2afd)

Address 0x60f000000130 is a wild pointer.
SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/avc_ext.c:2490 in gf_isom_dovi_config_get
Shadow bytes around the buggy address:
  0x0c1e7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1e7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1e7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1e7fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c1e7fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
=>0x0c1e7fff8020: fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1e7fff8070: 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
==2235126==ABORTING
```

source code

```
GF_DOVIDecoderConfigurationRecord *gf_isom_dovi_config_get(GF_ISOFile* the_file, u32 trackNumber, u32 DescriptionIndex)
{
    GF_TrackBox* trak;
    GF_MPEGVisualSampleEntryBox *entry;
    trak = gf_isom_get_track_from_file(the_file, trackNumber);
    if (!trak || !trak->Media || !DescriptionIndex) return NULL;
    entry = (GF_MPEGVisualSampleEntryBox*)gf_list_get(trak->Media->information->sampleTable->SampleDescription->child_boxes, DescriptionIndex - 1);
    if (!entry) return NULL;
    if (entry->internal_type != GF_ISOM_SAMPLE_ENTRY_VIDEO) return NULL;
    if (!entry->dovi_config) return NULL;          /**here**/
    return DOVI_DuplicateConfig(&entry->dovi_config->DOVIConfig);
}
```

sample poc:

poc1.zip

ps: it is similar with the issue which occured in older gpac version (#1846) . The bug was not patched . It still occured in the newest version.

Janette88 changed the title ~~heap-buffer-overflow in gf_isom_dovi_config_get of gpac2.0~~ heap-buffer-overflow in function gf_isom_dovi_config_get on Jul 5

Janette88 mentioned this issue on Jul 12

Heap Use After Free in function gf_isom_dovi_config_get #2220

Closed

3 tasks

jeanlf closed this as completed in `fef6242` on Jul 12

jeanlf mentioned this issue on Jul 12

Segmentation fault in DOVI_DuplicateConfig at isomedia/avc_ext.c:1479 #2219

Closed

3 tasks

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant