New issue

Jump to bottom

AddressSanitizer: heap-buffer-overflow media_tools/mpegts.c:1471 in gf_m2ts_section_complete #1422

Closed 3 tasks done **dr3dd589** opened this issue on Mar 1, 2020 · 0 comments

dr3dd589 commented on Mar 1, 2020

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

- [x] I looked for a similar issue and couldn't find any.
- [x] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
- [x] 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/

System info:
Ubuntu 18.04.6 LTS, X64, gcc version 7.4.0, gpac (latest master 4a7a63)

Compile Command:

```
$ CC="gcc -fsanitize=address -g" CXX="g++ -fsanitize=address -g" ./configure --static-mp4box
$ make
```

Run Command:

```
./MP4Box -dash 1000 crash_2
```

ASAN info:

```
=================================================================
==12759==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000000d3 at pc 0x55feb146edf3 bp 0x7fff627852e0 sp 0x7fff627852d0
READ of size 1 at 0x6020000000d3 thread T0
    #0 0x55feb146edf2 in gf_m2ts_section_complete media_tools/mpegts.c:1471
    #1 0x55feb146f3ab in gf_m2ts_gather_section media_tools/mpegts.c:1740
    #2 0x55feb147524c in gf_m2ts_process_packet media_tools/mpegts.c:3440
    #3 0x55feb147524c in gf_m2ts_process_data media_tools/mpegts.c:3507
    #4 0x55feb1484886 in gf_m2ts_probe_file media_tools/mpegts.c:4641
    #5 0x55feb13ac7f0 in gf_dash_segmenter_probe_input media_tools/dash_segmenter.c:5505
    #6 0x55feb13d350a in gf_dasher_add_input media_tools/dash_segmenter.c:6669
    #7 0x55feb0faea6f in mp4boxMain /home/dr3dd/fuzzing/gpac/applications/mp4box/main.c:4704
    #8 0x7f1e4bd95b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #9 0x55feb0f9d7a9 in _start (/home/dr3dd/fuzzing/gpac/bin/gcc/MP4Box+0x1657a9)

0x6020000000d3 is located 0 bytes to the right of 3-byte region [0x6020000000d0,0x6020000000d3)
allocated by thread T0 here:
    #0 0x7f1e4ca1df40 in realloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdef40)
    #1 0x55feb146f309 in gf_m2ts_gather_section media_tools/mpegts.c:1730

SUMMARY: AddressSanitizer: heap-buffer-overflow media_tools/mpegts.c:1471 in gf_m2ts_section_complete
Shadow bytes around the buggy address:
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa 02 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff8010: fa fa 00 00 fa fa 00 00 fa fa[03]fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8060: 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
==12759==ABORTING
```

gdb Info:

```
Program received signal SIGSEGV, Segmentation fault.
0x0000555555d45a2d in gf_m2ts_process_pmt (ts=<optimized out>, pmt=<optimized out>, sections=<optimized out>,
    table_id=<optimized out>, ex_table_id=<optimized out>, version_number=<optimized out>,
    last_section_number=<optimized out>, status=<optimized out>) at media_tools/mpegts.c:2535
2535                            gf_list_add(pmt->program->streams, es);
(gdb) bt
#0  0x0000555555d45a2d in gf_m2ts_process_pmt (ts=<optimized out>, pmt=<optimized out>, sections=<optimized out>,
    table_id=<optimized out>, ex_table_id=<optimized out>, version_number=<optimized out>,
```

```
    last_section_number=<optimized out>, status=<optimized out>) at media_tools/mpegts.c:2535
#1  0x00005555555d35506 in gf_m2ts_section_complete (ts=ts@entry=0x5555562c5a40, sec=sec@entry=0x5555562d7440,
    ses=ses@entry=0x5555562d7390) at media_tools/mpegts.c:1610
#2  0x00005555555d3638a in gf_m2ts_gather_section (ts=ts@entry=0x5555562c5a40, sec=0x5555562d7440,
    ses=ses@entry=0x5555562d7390, data=0x7ffffffa6821 "", data@entry=0x7ffffffa681a "", data_size=<optimized out>,
    hdr=<optimized out>, hdr=<optimized out>) at media_tools/mpegts.c:1740
#3  0x00005555555d3f3be in gf_m2ts_process_packet (data=0x7ffffffa681a "", ts=0x5555562c5a40)
    at media_tools/mpegts.c:3446
#4  gf_m2ts_process_data (ts=ts@entry=0x5555562c5a40, data=data@entry=0x7ffffffa6700 "", data_size=<optimized out>)
    at media_tools/mpegts.c:3507
#5  0x00005555555d54ca1 in gf_m2ts_probe_file (fileName=<optimized out>) at media_tools/mpegts.c:4641
#6  0x00005555555bf0844 in gf_dash_segmenter_probe_input (io_dash_inputs=io_dash_inputs@entry=0x5555562c4978,
    nb_dash_inputs=nb_dash_inputs@entry=0x5555562c4980, idx=idx@entry=0) at media_tools/dash_segmenter.c:5505
#7  0x00005555555c2dabb in gf_dasher_add_input (dasher=0x5555562c4970, input=<optimized out>)
    at media_tools/dash_segmenter.c:6669
#8  0x00005555555c88f5 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at main.c:4704
#9  0x00007ffff722bb97 in __libc_start_main () from /lib/x86_64-linux-gnu/libc.so.6
#10 0x00005555555a3e0a in _start () at main.c:5985
```

here is crash file:
crash_2.zip

Thanks
dr3dd

aureliendavid closed this as completed in 8c5e847 on Mar 6, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant