New issue

Jump to bottom

# null pointer reference in gf_isom_get_media_data_size #1377

Closed **cuanduo** opened this issue on Jan 1, 2020 · 1 comment

**cuanduo** commented on Jan 1, 2020

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

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

MP42TS -src $POC -dst-file /dev/null
count_video.zip
asan output

```
root@ubuntu:/home/tim/gpac# ../gpac-asan/MP42TS -src crashes/count_video.mp4-signal1b-0x0 -dst-file /dev/null
AddressSanitizer:DEADLYSIGNAL
=================================================================
==112791==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x55e4a53e12e4 bp 0x602000000370 sp 0x7fffdb37dbe0 T0)
==112791==The signal is caused by a READ memory access.
==112791==Hint: address points to the zero page.
    #0 0x55e4a53e12e3 in gf_isom_get_media_data_size isomedia/isom_read.c:3312
    #1 0x55e4a5391fdd in fill_isom_es_ifce /home/tim/gpac-asan/applications/mp42ts/main.c:620
    #2 0x55e4a5391fdd in open_source /home/tim/gpac-asan/applications/mp42ts/main.c:1518
    #3 0x55e4a53836c0 in parse_args /home/tim/gpac-asan/applications/mp42ts/main.c:2260
    #4 0x55e4a53836c0 in main /home/tim/gpac-asan/applications/mp42ts/main.c:2465
    #5 0x7f9a8b98ab6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)
    #6 0x55e4a53899c9 in _start (/home/tim/gpac-asan/MP42TS+0x1249c9)
```

**aureliendavid** added a commit that referenced this issue on Jan 8, 2020

`very ugly 'fix' for broken m2ts inputs (#1378, #1377)` c7e46e9

**aureliendavid** mentioned this issue on Jan 8, 2020

**null pointer reference in gf_m2ts_stream_process_pmt** #1378

Closed

**aureliendavid** commented on Jan 8, 2020 Contributor

see #1378

**aureliendavid** closed this as completed on Jan 8, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants