New issue

Jump to bottom

null pointer reference in gf_m2ts_stream_process_pmt #1378

Closed **cuanduo** opened this issue on Jan 1, 2020 · 2 comments

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_video1.zip
asan output

```
root@ubuntu:/home/tim/gpac# ../gpac-asan/MP42TS -src crashes/count_video.mp4-signalb-0x198 -dst-file /dev/null
Setting up program ID 1 - send rates: PSI 200 ms PCR 100 ms - PCR offset 0
AddressSanitizer:DEADLYSIGNAL
=================================================================
==115151==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x558236d3d311 bp 0x6080000008a0 sp 0x7ffd7d124a70 T0)
==115151==The signal is caused by a READ memory access.
==115151==Hint: address points to the zero page.
    #0 0x558236d3d310 in gf_m2ts_stream_process_pmt media_tools/m2ts_mux.c:718
    #1 0x558236d4dfd1 in gf_m2ts_mux_table_update_bitrate media_tools/m2ts_mux.c:256
    #2 0x558236d4dfd1 in gf_m2ts_mux_update_config media_tools/m2ts_mux.c:2543
    #3 0x558236bcfffd in main /home/tim/gpac-asan/applications/mp42ts/main.c:2684
    #4 0x7ff116424b6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)
    #5 0x558236bd59c9 in _start (/home/tim/gpac-asan/MP42TS+0x1249c9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV media_tools/m2ts_mux.c:718 in gf_m2ts_stream_process_pmt
==115151==ABORTING
```

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

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

aureliendavid commented on Jan 8, 2020 Contributor

for this and #1377 my quick and dirty fix was to add a very ugly abort()

error handling is pretty terrible in mp42ts apart from a bunch of asserts (that are ignored when compiling in release mode), return values are rarely checked, etc.

the abort should prevent afl/asan to detect it as a bug, and since it should only happen on very broken files it's not the end of the world, but it's still pretty ugly

if anyone has a better fix be my guest - in the meantime i'm closing the issue, reopen if needed

aureliendavid closed this as completed on Jan 8, 2020

aureliendavid mentioned this issue on Jan 8, 2020

null pointer reference in gf_isom_get_media_data_size #1377

Closed

Beuc commented on Jan 17, 2020

Hi,

I though I'd mention that abort() leads to mostly the same vulnerability (denial of service, in particular for a service that links to libgpac.so).
See for instance https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9211

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants