New issue

Jump to bottom

AddressSanitizer: NULL pointer dereference in media_tools/dash_segmenter.c:5264 in gf_dash_segmenter_probe_input #1423

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

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_3
```

ASAN info:

```
=================================================================
==13768==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x562656a3daf0 bp 0x000000000001 sp 0x7ffee325fef0 T0)
==13768==The signal is caused by a READ memory access.
==13768==Hint: address points to the zero page.
    #0 0x562656a3daef in gf_dash_segmenter_probe_input media_tools/dash_segmenter.c:5264
    #1 0x562656a6350a in gf_dasher_add_input media_tools/dash_segmenter.c:6669
    #2 0x56265663ea6f in mp4boxMain /home/dr3dd/fuzzing/gpac/applications/mp4box/main.c:4704
    #3 0x7fab411e9b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #4 0x56265662d7a9 in _start (/home/dr3dd/fuzzing/gpac/bin/gcc/MP4Box+0x1657a9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV media_tools/dash_segmenter.c:5264 in gf_dash_segmenter_probe_input
==13768==ABORTING
```

gdb info:

```
(gdb) r -dash 1000 ~/gpac_poc/crash_3
Starting program: /home/dr3dd/fuzzing/gpac/bin/gcc/MP4Box -dash 1000 ~/gpac_poc/crash_2
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
0x00005555555bf408c 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:5264
5264                                if (esd && (esd->decoderConfig->objectTypeIndication == GPAC_OTI_VIDEO_HEVC || esd->decoderConfig->objectTypeIndication == GPAC_OTI_VIDEO_LHVC)
(gdb) bt
#0  0x00005555555bf408c 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:5264
#1  0x00005555555c2dabb in gf_dasher_add_input (dasher=0x5555562c4970, input=<optimized out>)
    at media_tools/dash_segmenter.c:6669
#2  0x00005555555c88f5 in mp4boxMain (argc=<optimized out>, argv=<optimized out>) at main.c:4704
#3  0x00007ffff722bb97 in __libc_start_main () from /lib/x86_64-linux-gnu/libc.so.6
#4  0x00005555555a3e0a in _start () at main.c:5985
(gdb)
```

Here is crash file:
crash_3.zip

Thanks
dr3dd

jeanlf added a commit that referenced this issue on Jun 11, 2020

`fixed potential crash - cf #1423` e90526f

jeanlf commented on Jun 11, 2020 Contributor

fixed, thanks for the report

jeanlf closed this as completed on Jun 11, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants