New issue

Jump to bottom

A NULL pointer dereference in the function gf_hinter_track_finalize in media_tools/isom_hinter.c:970 #1660

Closed **Clingto** opened this issue on Dec 15, 2020 · 0 comments

Clingto commented on Dec 15, 2020 • edited

System info:
Ubuntu 16.04.6 LTS, X64, gcc 5.4.0, gpac (latest master `c4f8bc6` and the latest V1.0.1 `d8538e8`)

Compile Command:

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

Run Command:

```
$ MP4Box -hint $gf_hinter_track_finalize-null-pointer -out /dev/null
```

POC file:
https://github.com/Clingto/POC/blob/master/gpac-MP4Box/gpac-c4f8bc6e_poc/gf_hinter_track_finalize-null-pointer

gdb info:

```
Program received signal SIGSEGV, Segmentation fault.
0x000000000060eab8 in gf_hinter_track_finalize ()
(gdb) bt
#0  0x000000000060eab8 in gf_hinter_track_finalize ()
#1  0x0000000000040ad7c in HintFile ()
#2  0x00000000004172b2 in mp4boxMain ()
#3  0x00007ffff6ec7840 in __libc_start_main (main=0x409dc0 <main>, argc=5, argv=0x7fffffffdf68, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>, stack_end=0x7fff
#4  0x0000000000409df9 in _start ()
```

ASAN info:

```
Hinting file with Path-MTU 1450 Bytes
Hinting track ID 1 - Type "avc1:avc1" (H264) - BW 3 kbps
ASAN:SIGSEGV
=================================================================
==20754==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000003 (pc 0x00000092e516 bp 0x7fffe5a7ede0 sp 0x7fffe5a79300 T0)
    #0 0x92e515 in gf_hinter_track_finalize media_tools/isom_hinter.c:970
    #1 0x418f85 in HintFile /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:1448
    #2 0x42bdc7 in mp4boxMain /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:6641
    #3 0x7fd6bcc3b83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #4 0x417638 in _start (/opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/build/bin/MP4Box+0x417638)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV media_tools/isom_hinter.c:970 gf_hinter_track_finalize
==20754==ABORTING
```

Addition: This bug was found with our fuzzer, which is based on AFL. Our fuzzer is developed by Yuanpingyu(cfenicey@gmail.com) 、Xiangkun Jia(xiangkun@iscas.ac.cn) 、Marsman1996(lqliuyuwei@outlook.com) and Yanhao.

jeanlf closed this as completed in `a4eb327` on Jan 4, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant