New issue

Jump to bottom

AddressSanitizer: heap-buffer-overflow in gp_rtp_builder_do_avc ietf/rtp_pck_mpeg4.c:436 #1662

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 latest V1.0.1 `d8538e8`)
I think it is probably due to an imcomplete fix of #1483

Compile Command:

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

Run Command:

```
$ MP4Box -hint $gp_rtp_builder_do_avc-hepo -out /dev/null
```

POC file:
https://github.com/Clingto/POC/blob/master/gpac-MP4Box/gpac-c4f8bc6e_poc/gp_rtp_builder_do_avc-hepo

ASAN info:

```
==39148==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000dca9 at pc 0x000000fe1693 bp 0x7ffc75309fc0 sp 0x7ffc75309fb0
READ of size 1 at 0x60300000dca9 thread T0
    #0 0xfe1692 in gp_rtp_builder_do_avc ietf/rtp_pck_mpeg4.c:436
    #1 0x92b813 in gf_hinter_track_process media_tools/isom_hinter.c:796
    #2 0x418d5d in HintFile /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:1446
    #3 0x42bdc7 in mp4boxMain /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:6641
    #4 0x7fac0705783f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #5 0x417638 in _start (/opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/build/bin/MP4Box+0x417638)

0x60300000dca9 is located 0 bytes to the right of 25-byte region [0x60300000dc90,0x60300000dca9)
allocated by thread T0 here:
    #0 0x7fac07fff602 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98602)
    #1 0x7b69e5 in Media_GetSample isomedia/media.c:573
    #2 0x7602dc in gf_isom_get_sample_ex isomedia/isom_read.c:1808
    #3 0x92b36d in gf_hinter_track_process media_tools/isom_hinter.c:721
    #4 0x418d5d in HintFile /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:1446
    #5 0x42bdc7 in mp4boxMain /opt/data/yyp/fuzzsequence/test/0-day/SRC_asan/applications/mp4box/main.c:6641
    #6 0x7fac0705783f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)

SUMMARY: AddressSanitizer: heap-buffer-overflow ietf/rtp_pck_mpeg4.c:436 gp_rtp_builder_do_avc
Shadow bytes around the buggy address:
  0x0c067fff9b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9b60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9b70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9b80: fa fa fa fa fa fa fa fa fa fa fa fa 00 00 04 fa
=>0x0c067fff9b90: fa fa 00 00 00[01]fa fa fd fd fd fa fa fa fd fd
  0x0c067fff9ba0: fd fa fa fa fd fd fd fa fa fa fd fd fd fa fa fa
  0x0c067fff9bb0: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x0c067fff9bc0: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
  0x0c067fff9bd0: fd fa fa fa fd fd fd fa fa fa fd fd fd fa fa fa
  0x0c067fff9be0: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==39148==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 `b15020f` 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