New issue

Jump to bottom

[BUG] heap buffer overflow in gp_rtp_builder_do_hevc #2173

Closed 3 tasks done **kdsjZh** opened this issue on Apr 16 · 0 comments

kdsjZh commented on Apr 16 • edited

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/

Describe the bug

There is a heap-overflow bug in gp_rtp_builder_do_hevc, can be triggered via MP4Box+ ASan

Step to reproduce

./configure --enable-sanitizer && make -j$(nproc)
./MP4Box -hint -out /dev/null poc

Sanitizer output

```
[iso file] Box "hvcC" (start 919) has 26 extra bytes
Hinting track ID 1 - Type "hvc1:hvc1" (H265) - BW 3 kbps
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
```

```
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 191 but only 3 bytes left in sample 11
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
```

```
[rtp hinter] Broken AVC nalu encapsulation: NALU size is 0, ignoring it
=================================================================
==2628578==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001f15 at pc
0x7f14c2411bf5 bp 0x7ffec49a0110 sp 0x7ffec49a0100
READ of size 1 at 0x602000001f15 thread T0
    #0 0x7f14c2411bf4 in gp_rtp_builder_do_hevc ietf/rtp_pck_mpeg4.c:594
    #1 0x7f14c29c1da6 in gf_hinter_track_process media_tools/isom_hinter.c:834
    #2 0x561e3a6f0d97 in HintFile /home/hzheng/real-validate/gpac/applications/mp4box/main.c:3613
    #3 0x561e3a6f857b in mp4boxMain /home/hzheng/real-
validate/gpac/applications/mp4box/main.c:6481
    #4 0x7f14bfb8b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #5 0x561e3a6d0aed in _start (/home/hzheng/real-validate/gpac/bin/gcc/MP4Box+0xa9aed)

0x602000001f15 is located 0 bytes to the right of 5-byte region [0x602000001f10,0x602000001f15)
allocated by thread T0 here:
    #0 0x7f14c58d9bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f14c268782d in Media_GetSample isomedia/media.c:623
    #2 0x7f14c25e6e5c in gf_isom_get_sample_ex isomedia/isom_read.c:1905
    #3 0x7f14c29c16bd in gf_hinter_track_process media_tools/isom_hinter.c:756
    #4 0x561e3a6f0d97 in HintFile /home/hzheng/real-validate/gpac/applications/mp4box/main.c:3613
    #5 0x561e3a6f857b in mp4boxMain /home/hzheng/real-
validate/gpac/applications/mp4box/main.c:6481
    #6 0x7f14bfb8b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow ietf/rtp_pck_mpeg4.c:594 in gp_rtp_builder_do_hevc
Shadow bytes around the buggy address:
  0x0c047fff8390: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff83a0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff83b0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff83c0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff83d0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff83e0: fa fa[05]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff83f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8400: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8410: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8420: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8430: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 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
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  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
  Left alloca redzone:     ca
  Right alloca redzone:    cb
```

```
  Shadow gap:              cc
==2628578==ABORTING
```

version

system: ubuntu 20.04.3 LTS
compiler: gcc 9.3.0
gpac version: latest commit `6dcba53`

```
MP4Box - GPAC version 2.1-DEV-rev114-g6dcba5347-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --enable-sanitizer
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF
GPAC_HAS_QJS GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D
```

Credit

Han Zheng
NCNIPC of China
Hexhive

POC

crash.zip

jeanlf closed this as completed in `1773b7a` on Apr 19

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant