There is a heap-buffer-overflow in the dump_data_hex function of box_dump.c:51 #1341

Closed **gutiniao** opened this issue on Nov 12, 2019 · 1 comment

gutiniao commented on Nov 12, 2019

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

[√] I looked for a similar issue and couldn't find any.
[√] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
[√] 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/

A crafted input will lead to crash in box_dump.c at gpac 0.8.0.
Triggered by
./MP4Box -diso POC -out /dev/null

Poc
003-heep-dump_data51

The ASAN information is as follows:

```
./MP4Box -diso 003-heep-dump_data51 -out /dev/null
[iso file] Box "avcC" (start 939) has 34 extra bytes
[iso file] Unknown box type 0000 in parent sinf
[iso file] Unknown box type 0000 in parent schi
[iso file] Box "tfhd" size 20 (start 2642) invalid (read 28)
[iso file] senc box without tenc, assuming MS smooth+piff
[isobmf] Failed to parse SENC box, invalid SAI size
[isobmf] Failed to parse SENC box, invalid SAI size
[iso file] Unknown top-level box type 00303030
[iso file] Incomplete box 00303030 - start 3467 size 808453500
[iso file] Incomplete file while reading for dump - aborting parsing
=================================================================
==5711==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x603000000990 at pc 0x563f30697440 bp 0x7ffd8a7496b0 sp 0x7ffd8a7496a0
READ of size 1 at 0x603000000990 thread T0
    #0 0x563f3069743f in dump_data_hex isomedia/box_dump.c:51
    #1 0x563f3069743f in senc_dump isomedia/box_dump.c:4823
    #2 0x563f306a06ad in gf_isom_box_dump_ex isomedia/box_funcs.c:1738
    #3 0x563f3067c5bc in gf_isom_box_dump isomedia/box_dump.c:97
    #4 0x563f3067c5bc in gf_isom_box_array_dump isomedia/box_dump.c:107
    #5 0x563f306a07cf in gf_isom_box_dump_done isomedia/box_funcs.c:1747
    #6 0x563f3068b939 in traf_dump isomedia/box_dump.c:2461
    #7 0x563f306a06ad in gf_isom_box_dump_ex isomedia/box_funcs.c:1738
    #8 0x563f3067c5bc in gf_isom_box_dump isomedia/box_dump.c:97
    #9 0x563f3067c5bc in gf_isom_box_array_dump isomedia/box_dump.c:107
    #10 0x563f306a07cf in gf_isom_box_dump_done isomedia/box_funcs.c:1747
    #11 0x563f3068b389 in moof_dump isomedia/box_dump.c:2431
    #12 0x563f306a06ad in gf_isom_box_dump_ex isomedia/box_funcs.c:1738
    #13 0x563f3067c7f3 in gf_isom_box_dump isomedia/box_dump.c:97
    #14 0x563f3067c7f3 in gf_isom_dump isomedia/box_dump.c:139
    #15 0x563f3041b734 in dump_isom_xml /home/liuz/gpac-master/applications/mp4box/filedump.c:1930
    #16 0x563f30405c92 in mp4boxMain /home/liuz/gpac-master/applications/mp4box/main.c:4982
    #17 0x7f6e421e6b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #18 0x563f303f2b19 in _start (/usr/local/gpac-asan3/bin/MP4Box+0x163b19)

0x603000000990 is located 0 bytes to the right of 32-byte region [0x603000000970,0x603000000990)
allocated by thread T0 here:
    #0 0x7f6e42e6fb50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x563f30b5ebe9 in senc_Parse isomedia/box_code_drm.c:1349

SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/box_dump.c:51 in dump_data_hex
Shadow bytes around the buggy address:
  0x0c067fff80e0: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
  0x0c067fff80f0: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
  0x0c067fff8100: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
  0x0c067fff8110: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
  0x0c067fff8120: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
=>0x0c067fff8130: 00 00[fa]fa 00 00 00 00 fa fa fd fd fd fd fa fa
  0x0c067fff8140: 00 00 00 00 fa fa fd fd fd fd fa fa fa fa fa fa
  0x0c067fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8170: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff8180: 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
==5711==ABORTING
```

aureliendavid added a commit that referenced this issue on Jan 9, 2020

`add IV_size check on senc_Parse (#1341, #1342)` a0e6aa8

aureliendavid commented on Jan 9, 2020 Contributor

thanks for the report

this should be fixed by the commit above

reopen if needed

aureliendavid closed this as completed on Jan 9, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants