New issue

Jump to bottom

There is a heap-buffer-overflow in the GetGhostNum function of stbl_read.c:369 #1344

Closed **gutiniao** opened this issue on Nov 13, 2019 · 1 comment

gutiniao commented on Nov 13, 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 stbl_read.c at gpac 0.8.0.

Triggered by
./MP4Box -diso POC -out /dev/null

Poc
006GetGhostNum-heap

The ASAN information is as follows:

```
./MP4Box -diso 006GetGhostNum-heap -out /dev/null
[iso file] Box "avcC" (start 939) has 34 extra bytes
[iso file] Unknown box type 0000 in parent sinf
[iso file] Box "dref" (start 1403) has 4 extra bytes
[iso file] Missing DataInformationBox
[iso file] Box "minf" (start 1371) has 291 extra bytes
[iso file] Track with no sample table !
[iso file] Track with no sample description box !
=================================================================
==7153==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000454 at pc 0x5572c94aafff bp 0x7fff10f02f50 sp 0x7fff10f02f40
READ of size 4 at 0x602000000454 thread T0
    #0 0x5572c94aaffe in GetGhostNum isomedia/stbl_read.c:369
    #1 0x5572c94aaffe in stbl_GetSampleInfos isomedia/stbl_read.c:436
    #2 0x5572c943e253 in gf_isom_get_sample_cenc_info_ex isomedia/isom_read.c:4153
    #3 0x5572c98c8c2f in senc_Parse isomedia/box_code_drm.c:1353
    #4 0x5572c94203e6 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:399
    #5 0x5572c9422bca in gf_isom_open_file isomedia/isom_intern.c:615
    #6 0x5572c916b852 in mp4boxMain /home/liuz/gpac-master/applications/mp4box/main.c:4767
    #7 0x7f0e00306b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x5572c915cb19 in _start (/usr/local/gpac-asan3/bin/MP4Box+0x163b19)

0x602000000454 is located 3 bytes to the right of 1-byte region [0x602000000450,0x602000000451)
allocated by thread T0 here:
    #0 0x7f0e00f8fb50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x5572c98a424a in stsc_Read isomedia/box_code_base.c:5734

SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/stbl_read.c:369 in GetGhostNum
Shadow bytes around the buggy address:
  0x0c047fff8030: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 01 fa
  0x0c047fff8040: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8050: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8060: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8070: fa fa 00 00 fa fa 00 00 fa fa fd fd fa fa fd fd
=>0x0c047fff8080: fa fa 00 00 fa fa 01 fa fa fa[01]fa fa fa 00 00
  0x0c047fff8090: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 01 fa
  0x0c047fff80a0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff80b0: fa fa 00 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff80c0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 01 fa
  0x0c047fff80d0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 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
==7153==ABORTING
```

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

fix for stsc boxes with 0 entries (#1344) 5aa8c4b

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