New issue

Jump to bottom

BUG: heap-buffer-overflow in MP4Box at src/isomedia/schm_box_size:179 #1879

Closed   3 tasks done   **AntsKnows** opened this issue on Aug 18, 2021 · 0 comments

AntsKnows commented on Aug 18, 2021 • edited

- ☑ 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 ...).

It's a heap-buffer-overflow bug caused by missing '\0' check of the end of URI.

Step to reproduce:
1.get latest commit code (MP4Box - GPAC version 1.1.0-DEV-rev1169-gbbd741e-master)
2.compile with --enable-sanitizer
3.run ./MP4BOX -hint poc -out /dev/null

Env:
Ubunut 20.04 , clang 10.0.0

ASAN report

```
==789683==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x604000000bb7 at pc 0x7f277ca50a6d bp 0x7ffd14f790b0 sp 0x7ffd14f78858
READ of size 40 at 0x604000000bb7 thread T0
    #0 0x7f277ca50a6c  (/lib/x86_64-linux-gnu/libasan.so.5+0x67a6c)
    #1 0x7f277a6d0ece in schm_box_size isomedia/box_code_drm.c:179
    #2 0x7f277a7569f1 in gf_isom_box_size_listing isomedia/box_funcs.c:1903
    #3 0x7f277a7569f1 in gf_isom_box_size isomedia/box_funcs.c:1915
    #4 0x7f277a805c14 in WriteInterleaved isomedia/isom_store.c:1870
    #5 0x7f277a8086d3 in WriteToFile isomedia/isom_store.c:2527
    #6 0x7f277a7a73d9 in gf_isom_write isomedia/isom_read.c:600
    #7 0x7f277a7a778f in gf_isom_close isomedia/isom_read.c:624
    #8 0x562161c082db in mp4boxMain /home/lly/pro/gpac_public/applications/mp4box/main.c:6401
    #9 0x7f27799da0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #10 0x562161bd2bdd in _start (/home/lly/pro/gpac_public/bin/gcc/MP4Box+0x4abdd)

0x604000000bb7 is located 0 bytes to the right of 39-byte region [0x604000000b90,0x604000000bb7)
allocated by thread T0 here:
    #0 0x7f277caf6bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f277a6d08b7 in schm_box_read isomedia/box_code_drm.c:148

SUMMARY: AddressSanitizer: heap-buffer-overflow (/lib/x86_64-linux-gnu/libasan.so.5+0x67a6c)
Shadow bytes around the buggy address:
  0x0c087fff8120: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff8130: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fa
  0x0c087fff8140: fa fa fd fd fd fd fd fd fa fa 00 00 00 00 00 01
  0x0c087fff8150: fa fa 00 00 00 00 04 fa fa fa 00 00 00 00 05 fa
  0x0c087fff8160: fa fa 00 00 00 00 00 06 fa fa 00 00 00 00 02 fa
=>0x0c087fff8170: fa fa 00 00 00 00[07]fa fa fa 00 00 00 00 00 00
  0x0c087fff8180: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c087fff8190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff81a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff81b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
```

Buggy code and reason:

```
GF_Err schm_box_size(GF_Box *s)
{
        GF_SchemeTypeBox *ptr = (GF_SchemeTypeBox *) s;
        if (!s) return GF_BAD_PARAM;
        ptr->size += 8;
        if (ptr->flags & 0x000001) ptr->size += 1 + (ptr->URI ? strlen(ptr->URI) : 0);   <---strlen overflow once URI does not end with '\0'
        return GF_OK;
}
```

poc.zip

AntsKnows changed the title ~~heap-buffer-overflow in schm_box_size~~ **BUG: heap-buffer-overflow in schm_box_size** on Aug 19, 2021

AntsKnows changed the title ~~BUG: heap-buffer-overflow in schm_box_size~~ **BUG: heap-buffer-overflow in MP4Box at src/isomedia/schm_box_size:179** on Aug 27, 2021

jeanlf closed this as completed in f196689 on Aug 30, 2021

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant