New issue

Jump to bottom

A heap-buffer-overflow in function gp_rtp_builder_do_mpeg12_video #1838

Closed **dhbbb** opened this issue on Jul 2, 2021 · 0 comments

dhbbb commented on Jul 2, 2021

Hello,
A heap-buffer-overflow has occurred when running program MP4Box,this can reproduce on the lattest commit.
System info：
Ubuntu 20.04.1 : clang 10.0.0 , gcc 9.3.0

poc1.zip

Verification steps：
1.Get the source code of gpac
2.Compile

```
cd gpac-master
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" ./configure
make
```

3.run MP4Box

```
./MP4Box -hint poc -out /dev/null
```

asan info

```
=================================================================
==2631249==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001bd4 at pc 0x7f2ac7fe5b9b bp 0x7ffc4389ba70 sp 0x7ffc4389ba60
READ of size 1 at 0x602000001bd4 thread T0
    #0 0x7f2ac7fe5b9a in gp_rtp_builder_do_mpeg12_video ietf/rtp_pck_mpeg12.c:156
    #1 0x7f2ac889948a in gf_hinter_track_process media_tools/isom_hinter.c:808
    #2 0x559f0eb8ae2b in HintFile /home/.../gpac/gpac-master/applications/mp4box/main.c:3499
    #3 0x559f0eba1d54 in mp4boxMain /home/.../gpac/gpac-master/applications/mp4box/main.c:6297
    #4 0x7f2ac74d10b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #5 0x559f0eb54f1d in _start (/home/.../gpac/gpac-master/bin/gcc/MP4Boxfl+0x48f1d)

0x602000001bd4 is located 0 bytes to the right of 4-byte region [0x602000001bd0,0x602000001bd4)
allocated by thread T0 here:
    #0 0x7f2aca3afbc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f2ac83d56cd in Media_GetSample isomedia/media.c:617

SUMMARY: AddressSanitizer: heap-buffer-overflow ietf/rtp_pck_mpeg12.c:156 in gp_rtp_builder_do_mpeg12_video
Shadow bytes around the buggy address:
  0x0c047fff8320: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8330: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8340: fa fa fd fd fa fa fd fd fa fa fd fa fa fa 00 00
  0x0c047fff8350: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8360: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff8370: fa fa 00 00 fa fa 00 00 fa fa[04]fa fa fa fa fa
  0x0c047fff8380: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8390: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff83a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff83b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff83c0: 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
==2631249==ABORTING
```

source code of rtp_pck_mpeg12.c

```
143 max_pck_size = builder->Path_MTU - 4;
144
145     payload = data + offset;
146     pic_type = (payload[1] >> 3) & 0x7;
147     /*first 6 bits (MBZ and T bit) not used*/
148     /*temp ref on 10 bits*/
149     mpv_hdr[0] = (payload[0] >> 6) & 0x3;
150     mpv_hdr[1] = (payload[0] << 2) | ((payload[1] >> 6) & 0x3);
151     mpv_hdr[2] = pic_type;
152     mpv_hdr[3] = 0;
153
154     if ((pic_type==2) || (pic_type== 3)) {
155             mpv_hdr[3] = (u8) ((((u32)payload[3]) << 5) & 0xf);
```

```
            if ((payload[4] & 0x80) != 0) mpv_hdr[3] |= 0x10;
            if (pic_type == 3) mpv_hdr[3] |= (payload[4] >> 3) & 0xf;
    }
```

jeanlf closed this as completed in 8281884 on Jul 5, 2021

jeanlf mentioned this issue on Jul 5, 2021

A heap-buffer-overflow in rtp_pck_mpeg12.c #1839

Closed

attritionorg mentioned this issue on Aug 19, 2021

Bug: heap-buffer-overflow in gp_rtp_builder_do_mpeg12_video #1881

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant