gpac / gpac Public

Code Issues 10 Pull requests 2 Wiki Security Insights

New issue

Jump to bottom

heap-buffer-overflow in gp_rtp_builder_do_tx3g #1842

Closed dhbbb opened this issue on Jul 5, 2021 · 1 comment

dhbbb commented on Jul 5, 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

```
=================================================================
==47156==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001892 at pc 0x7f5f1dea9b2c bp 0x7ffe02fd8810 sp 0x7ffe02fd8800
READ of size 1 at 0x602000001892 thread T0
    #0 0x7f5f1dea9b2b in gp_rtp_builder_do_tx3g ietf/rtp_pck_3gpp.c:399
    #1 0x7f5f1e76148a in gf_hinter_track_process media_tools/isom_hinter.c:808
    #2 0x5622a222ce2b in HintFile /home/.../gpac/gpac-master/applications/mp4box/main.c:3499
    #3 0x5622a2243d54 in mp4boxMain /home/.../gpac/gpac-master/applications/mp4box/main.c:6297
    #4 0x7f5f1d3990b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #5 0x5622a21f6f1d in _start (/home/.../gpac/gpac-master/bin/gcc/MP4Box+0x48f1d)

0x602000001892 is located 0 bytes to the right of 2-byte region [0x602000001890,0x602000001892)
allocated by thread T0 here:
    #0 0x7f5f20277bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7f5f1e29d6cd in Media_GetSample isomedia/media.c:617

SUMMARY: AddressSanitizer: heap-buffer-overflow ietf/rtp_pck_3gpp.c:399 in gp_rtp_builder_do_tx3g
Shadow bytes around the buggy address:
  0x0c047fff82c0: fa fa fd fd fa fa 00 00 fa fa 00 00 fa fa fd fd
  0x0c047fff82d0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff82e0: fa fa fd fa fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff82f0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8300: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff8310: fa fa[02]fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8330: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8340: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8350: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8360: 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
==47156==ABORTING
```

source code

```
396     pay_start = 2;
397     if (txt_size>2) {
398             /*seems 3GP only accepts BE UTF-16 (no LE, no UTF32)*/
399             if (((u8) data[2]==(u8) 0xFE) && ((u8) data[3]==(u8) 0xFF)) {
400                     is_utf_16 = GF_TRUE;
401                     pay_start = 4;
402                     txt_size -= 2;
403             }
404     }
405     samp_size = data_size - pay_start;
```

jeanlf closed this as completed in 13442ec on Jul 6, 2021

dhbbb commented on Aug 5, 2021 Author

This is CVE-2021-36584

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant