New issue

Jump to bottom

[security]heap buffer overlow in MP4Box print_udta #1765

Closed **5n1p3r0010** opened this issue on Apr 29, 2021 · 0 comments

5n1p3r0010 commented on Apr 29, 2021

Hi,

There is a heap buffer overflow issue in gpac MP4Box print_udta,this can reproduce on the lattest commit.

Steps To Reproduce

build:

```
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --enable-debug
make
```

run as:

```
MP4Box -info <poc>
```

shows the following log:

```
=================================================================
==3138155==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000001dc6 at pc 0x7fcee1b21dbb bp 0x7ffedaaa00b0 sp 0x7ffedaa9f828
READ of size 1095 at 0x619000001dc6 thread T0
    #0 0x7fcee1b21dba  (/lib/x86_64-linux-gnu/libasan.so.5+0x9cdba)
    #1 0x7fcee1b22fa6 in vfprintf (/lib/x86_64-linux-gnu/libasan.so.5+0x9dfa6)
    #2 0x7fcee1b230ae in __interceptor_fprintf (/lib/x86_64-linux-gnu/libasan.so.5+0x9e0ae)
    #3 0x55cca7eb582c in print_udta /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:1903
    #4 0x55cca7ebe071 in DumpMovieInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:3587
    #5 0x55cca7eab8f5 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5904
    #6 0x55cca7ead653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6335
    #7 0x7fcee0eeb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x55cca7e992ad in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x182ad)

0x619000001dc6 is located 0 bytes to the right of 1094-byte region [0x619000001980,0x619000001dc6)
allocated by thread T0 here:
    #0 0x7fcee1b92bc8 in malloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10dbc8)
    #1 0x7fcee11660f0 in gf_malloc utils/alloc.c:150
    #2 0x7fcee1375ba9 in gf_isom_get_user_data isomedia/isom_read.c:2683
    #3 0x55cca7eb57c4 in print_udta /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:1896
    #4 0x55cca7ebe071 in DumpMovieInfo /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/filedump.c:3587
    #5 0x55cca7eab8f5 in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5904
    #6 0x55cca7ead653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6335
    #7 0x7fcee0eeb0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/lib/x86_64-linux-gnu/libasan.so.5+0x9cdba)
Shadow bytes around the buggy address:
  0x0c327fff8360: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8370: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8380: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8390: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff83a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff83b0: 00 00 00 00 00 00 00 00[06]fa fa fa fa fa fa fa
  0x0c327fff83c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff83d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff83e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff83f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8400: 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
==3138155==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
heap-overflow_print_udta.zip

jeanlf closed this as completed in eb71812 on Apr 30, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant