gpac / **gpac** Public

Code Issues 10 Pull requests 2 Wiki Security Insights

New issue

Jump to bottom

heap-buffer-overflow isomedia/box_funcs.c:2074 in gf_isom_box_dump_start_ex #2280

Closed **17ssDP** opened this issue on Oct 9 · 0 comments

17ssDP commented on Oct 9

Description

Heap-buffer-overflow in isomedia/box_funcs.c:2074 in gf_isom_box_dump_start_ex

Version

```
$ ./MP4Box -version
MP4Box - GPAC version 2.1-DEV-rev368-gfd054169b-master
(c) 2000-2022 Telecom Paris distributed under LGPL v2.1+ - http://gpac.io

Please cite our work in your research:
        GPAC Filters: https://doi.org/10.1145/3339825.3394929
        GPAC: https://doi.org/10.1145/1291233.1291452

GPAC Configuration: --enable-sanitizer
Features: GPAC_CONFIG_LINUX GPAC_64_BITS GPAC_HAS_IPV6 GPAC_HAS_SOCK_UN GPAC_MINIMAL_ODF
GPAC_HAS_QJS GPAC_HAS_JPEG GPAC_HAS_PNG GPAC_HAS_LINUX_DVB  GPAC_DISABLE_3D
```

Replay

```
git clone https://github.com/gpac/gpac.git
cd gpac
./configure --enable-sanitizer
make -j$(nproc)
./bin/gcc/MP4Box -diso mp4box-diso-heap-buffer-over-flow-1
```

POC

https://github.com/17ssDP/fuzzer_crashes/blob/main/gpac/mp4box-diso-heap-buffer-over-flow-1

ASAN

```
[iso file] Read Box type 04@0004 (0x04400004) at position 94 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "meta" (start 32) has 206 extra bytes
[iso file] Box "uuid" (start 4061) has 58 extra bytes
[iso file] Incomplete box mdat - start 4151 size 54847
[iso file] Incomplete file while reading for dump - aborting parsing
=================================================================
==18099==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x604000000540 at pc
0x7f54a04dd880 bp 0x7ffcec3ea7e0 sp 0x7ffcec3ea7d0
READ of size 1 at 0x604000000540 thread T0
    #0 0x7f54a04dd87f in gf_isom_box_dump_start_ex isomedia/box_funcs.c:2074
    #1 0x7f54a04dd87f in gf_isom_box_dump_start isomedia/box_funcs.c:2093
    #2 0x7f54a04c0ae7 in trgt_box_dump isomedia/box_dump.c:5807
    #3 0x7f54a04ddbb8 in gf_isom_box_dump isomedia/box_funcs.c:2108
    #4 0x7f54a0470ffa in gf_isom_box_array_dump isomedia/box_dump.c:104
    #5 0x7f54a04ddda8 in gf_isom_box_dump_done isomedia/box_funcs.c:2115
    #6 0x7f54a04c09d5 in trgr_box_dump isomedia/box_dump.c:5799
    #7 0x7f54a04ddbb8 in gf_isom_box_dump isomedia/box_funcs.c:2108
    #8 0x7f54a04714d6 in gf_isom_dump isomedia/box_dump.c:138
    #9 0x55e8639f1804 in dump_isom_xml /home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/applications/mp4box/filedump.c:2067
    #10 0x55e8639c1d79 in mp4box_main /home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/applications/mp4box/mp4box.c:6364
    #11 0x7f549f4e0c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #12 0x55e8639920a9 in _start (/home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/bin/gcc/MP4Box+0x4e0a9)

0x604000000540 is located 0 bytes to the right of 48-byte region [0x604000000510,0x604000000540)
allocated by thread T0 here:
    #0 0x7f54a2a4cb40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7f54a041bd12 in trgt_box_new isomedia/box_code_base.c:10623

SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/box_funcs.c:2074 in
gf_isom_box_dump_start_ex
Shadow bytes around the buggy address:
  0x0c087fff8050: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c087fff8060: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 fa
  0x0c087fff8070: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 fa
  0x0c087fff8080: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c087fff8090: fa fa fd fd fd fd fd fd fa fa 00 00 00 00 00 00
=>0x0c087fff80a0: fa fa 00 00 00 00 00 00[fa]fa fa fa fa fa fa fa
  0x0c087fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff80f0: 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
==18099==ABORTING
```

Environment

```
Ubuntu 16.04
Clang 10.0.1
gcc 5.5
```

jeanlf closed this as completed in `f17dae3` on Oct 10

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant