New issue

Jump to bottom

# heap-buffer-overflow isomedia/isom_intern.c:227 in FixSDTPInTRAF #2278

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

**17ssDP** commented on Oct 9

## Description

Heap-buffer-overflow in isomedia/isom_intern.c:227 in FixSDTPInTRAF

## 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 -bt mp4box-bt-heap-buffer-over-flow-0
```

## POC

https://github.com/17ssDP/fuzzer_crashes/blob/main/gpac/mp4box-bt-heap-buffer-over-flow-0

## ASAN

```
[iso file] Unknown box type sjhm in parent sinf
[iso file] Unknown box type sgp00 in parent stbl
[iso file] Read Box type 00000000 (0x00000000) at position 2168 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "traf" (start 2028) has 458 extra bytes
[iso file] Unknown box type shgp in parent traf
=================================================================
==31145==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000001914 at pc
0x7fe0339cbbf8 bp 0x7ffc2041a330 sp 0x7ffc2041a320
READ of size 1 at 0x602000001914 thread T0
    #0 0x7fe0339cbbf7 in FixSDTPInTRAF isomedia/isom_intern.c:227
    #1 0x7fe0339cbbf7 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:663
    #2 0x7fe0339ce0e5 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:866
    #3 0x7fe0339ce0e5 in gf_isom_open_file isomedia/isom_intern.c:986
    #4 0x55ec82396048 in mp4box_main /home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/applications/mp4box/mp4box.c:6175
    #5 0x7fe032987c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #6 0x55ec823690a9 in _start (/home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/bin/gcc/MP4Box+0x4e0a9)

0x602000001914 is located 0 bytes to the right of 4-byte region [0x602000001910,0x602000001914)
allocated by thread T0 here:
    #0 0x7fe035ef3b40 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb40)
    #1 0x7fe0338a4541 in sdtp_box_read isomedia/box_code_base.c:8354

SUMMARY: AddressSanitizer: heap-buffer-overflow isomedia/isom_intern.c:227 in FixSDTPInTRAF
Shadow bytes around the buggy address:
  0x0c047fff82d0: fa fa 00 00 fa fa 00 00 fa fa 01 fa fa fa 00 00
  0x0c047fff82e0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa fd fa
  0x0c047fff82f0: fa fa 00 00 fa fa 00 00 fa fa 00 00 fa fa 00 00
  0x0c047fff8300: fa fa 00 fa fa fa 00 00 fa fa 00 07 fa fa 00 00
  0x0c047fff8310: fa fa 00 fa fa fa 00 00 fa fa 00 00 fa fa 00 00
=>0x0c047fff8320: fa fa[04]fa fa fa 00 00 fa fa 00 00 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
  0x0c047fff8370: 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
==31145==ABORTING
```

## Environment

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

 **jeanlf** closed this as completed in `3661da2` on Oct 10

---

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant