New issue

Jump to bottom

SEGV isomedia/meta.c:177 in gf_isom_get_meta_item_info #2282

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

17ssDP commented on Oct 9

Description

SEGV in isomedia/meta.c:177 in gf_isom_get_meta_item_info

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 -info mp4box-info-segv-1
```

POC

https://github.com/17ssDP/fuzzer_crashes/blob/main/gpac/mp4box-info-segv-1

ASAN

```
[iso file] Unknown box type i000000 in parent iinf
[iso file] Unknown top-level box type v000000
[iso file] Incomplete box v000000 - start 308 size 191662031
[iso file] Incomplete file while reading for dump - aborting parsing
# File Meta type: "Meta" - 3 resource item(s)
ASAN:DEADLYSIGNAL
=================================================================
==52314==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x7f4d67b428f9 bp
0x000000000000 sp 0x7ffcd749c3c0 T0)
==52314==The signal is caused by a READ memory access.
==52314==Hint: address points to the zero page.
    #0 0x7f4d67b428f8 in gf_isom_get_meta_item_info isomedia/meta.c:177
    #1 0x55fa2660a89e in DumpMetaItem /gpac/applications/mp4box/filedump.c:2467
    #2 0x55fa26642cc8 in DumpMovieInfo /gpac/applications/mp4box/filedump.c:3820
    #3 0x55fa265efee4 in mp4box_main /gpac/applications/mp4box/mp4box.c:6359
    #4 0x7f4d669cfc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #5 0x55fa265c00a9 in _start (/gpac/bin/gcc/MP4Box+0x4e0a9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/meta.c:177 in gf_isom_get_meta_item_info
==52314==ABORTING
```

Environment

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

jeanlf closed this as completed in `8a0e8e4` on Oct 10

Assignees

No one assigned

Labels

None yet

Projects

None vet

No labels yet

Milestone

No milestone

Development

No branches or pull requests

---

1 participant