New issue

Jump to bottom

# SEGV isomedia/meta.c:1929 in gf_isom_meta_restore_items_ref #2281

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

17ssDP commented on Oct 9

## Description

SEGV in isomedia/meta.c:1929 in gf_isom_meta_restore_items_ref

## 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-0
```

## POC

https://github.com/17ssDP/fuzzer_crashes/blob/main/gpac/mp4box-info-segv-0

## ASAN

```
[iso file] Read Box type 0003E8d (0x0003E864) at position 653 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Missing DataInformationBox
[iso file] Box "minf" (start 645) has 3400 extra bytes
[iso file] Track with no sample table !
[iso file] Track with no sample description box !
[isom] not enough bytes in box A9too: 29 left, reading 41 (file isomedia/box_code_apple.c, line
117)
[iso file] Read Box "A9too" (start 4122) failed (Invalid IsoMedia File) - skipping
[iso file] Read Box "ilst" (start 4114) failed (Invalid IsoMedia File) - skipping
[iso file] Read Box type 000000! (0x00000021) at position 4077 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "meta" (start 4069) has 74 extra bytes
ASAN:DEADLYSIGNAL
=================================================================
==57686==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000002c (pc 0x7fb4c621a438 bp
0x000000000000 sp 0x7fff370fe330 T0)
==57686==The signal is caused by a READ memory access.
==57686==Hint: address points to the zero page.
    #0 0x7fb4c621a437 in gf_isom_meta_restore_items_ref isomedia/meta.c:1929
    #1 0x7fb4c60c4127 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:429
    #2 0x7fb4c60d00e5 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:866
    #3 0x7fb4c60d00e5 in gf_isom_open_file isomedia/isom_intern.c:986
    #4 0x5627a34e0048 in mp4box_main /gpac/applications/mp4box/mp4box.c:6175
    #5 0x7fb4c5089c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #6 0x5627a34b30a9 in _start (/gpac/bin/gcc/MP4Box+0x4e0a9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/meta.c:1929 in gf_isom_meta_restore_items_ref
==57686==ABORTING
```

## Environment

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

**jeanlf** closed this as completed in `62dbd5c` on Oct 10

Assignees

No one assigned

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant