New issue

Jump to bottom

SEGV BD_CheckSFTimeOffset bifs/field_decode.c:58 #2276

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

17ssDP commented on Oct 9

Description

SEGV in BD_CheckSFTimeOffset bifs/field_decode.c:58

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-segv-0
```

POC

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

ASAN

```
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent minf
[iso file] Missing DataInformationBox
[iso file] Unknown box type 0000 in parent moov
[iso file] Read Box type 0000 (0x30303030) at position 11542 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "moov" (start 20) has 806 extra bytes
[iso file] Unknown top-level box type 0000
[iso file] Incomplete box 0000 - start 12356 size 808358436
[iso file] Incomplete file while reading for dump - aborting parsing
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent moov
[iso file] Unknown box type 0000 in parent minf
[iso file] Missing DataInformationBox
[iso file] Unknown box type 0000 in parent moov
[iso file] Read Box type 0000 (0x30303030) at position 11542 has size 0 but is not at root/file
level. Forbidden, skipping end of parent box !
[iso file] Box "moov" (start 20) has 806 extra bytes
[iso file] Unknown top-level box type 0000
[iso file] Incomplete box 0000 - start 12356 size 808358436
[iso file] Incomplete file while reading for dump - aborting parsing
MPEG-4 BIFS Scene Parsing
[ODF] Reading bifs config: shift in sizes (not supported)
ASAN:DEADLYSIGNAL                | (00/100)
=================================================================
==64022==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000001 (pc 0x7f4bf2457608 bp
0x7fff7805fc00 sp 0x7fff7805f360 T0)
==64022==The signal is caused by a READ memory access.
==64022==Hint: address points to the zero page.
    #0 0x7f4bf2457607  (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x5b607)
    #1 0x7f4befd4dd1a in BD_CheckSFTimeOffset bifs/field_decode.c:58
    #2 0x7f4befd53e80 in gf_bifs_dec_sf_field bifs/field_decode.c:105
    #3 0x7f4befd6a1be in BM_XReplace bifs/memory_decoder.c:355
    #4 0x7f4befd6a1be in BM_ParseExtendedUpdates bifs/memory_decoder.c:398
    #5 0x7f4befd754ad in BM_ParseInsert bifs/memory_decoder.c:586
    #6 0x7f4befd754ad in BM_ParseCommand bifs/memory_decoder.c:908
    #7 0x7f4befd7660d in gf_bifs_decode_command_list bifs/memory_decoder.c:1038
    #8 0x7f4bf0743bc6 in gf_sm_load_run_isom scene_manager/loader_isom.c:303
    #9 0x562cf53f8dd7 in dump_isom_scene /home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/applications/mp4box/filedump.c:207
    #10 0x562cf53d37ff in mp4box_main /home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/applications/mp4box/mp4box.c:6336
    #11 0x7f4beef6ec86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
```

```
    #12 0x562cf53a50a9 in _start (/home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/bin/gcc/MP4Box+0x4e0a9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/usr/lib/x86_64-linux-gnu/libasan.so.4+0x5b607)
==64022==ABORTING
```

Environment

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

jeanlf closed this as completed in `6bff06c` on Oct 10

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant