gpac / **gpac** Public

Code Issues 10 Pull requests 2 Wiki Security Insights

New issue

Jump to bottom

SEGV scene_manager/scene_dump.c:693 in gf_dump_vrml_sffield #2277

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

17ssDP commented on Oct 9

Description

SEGV scene_manager/scene_dump.c:693 in gf_dump_vrml_sffield

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-1
```

POC

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

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)
[MP4 Loading] Unable to fetch sample 38 from track ID 8 - aborting track import
Scene loaded - dumping 1 systems streams
ASAN:DEADLYSIGNAL
=================================================================
==42376==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x7f6a20c34c94 bp
0x60b000000720 sp 0x7ffd44396130 T0)
==42376==The signal is caused by a READ memory access.
==42376==Hint: address points to the zero page.
    #0 0x7f6a20c34c93 in gf_dump_vrml_sffield scene_manager/scene_dump.c:693
    #1 0x7f6a20c69012 in gf_dump_vrml_simple_field scene_manager/scene_dump.c:775
    #2 0x7f6a20c5020c in DumpXReplace scene_manager/scene_dump.c:2291
    #3 0x7f6a20c5020c in gf_sm_dump_command_list scene_manager/scene_dump.c:2901
    #4 0x7f6a20c77d57 in gf_sm_dump scene_manager/scene_dump.c:3519
    #5 0x556786082cef in dump_isom_scene /home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/applications/mp4box/filedump.c:221
    #6 0x55678605d7ff in mp4box_main /home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/applications/mp4box/mp4box.c:6336
    #7 0x7f6a1f3bac86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #8 0x55678602f0a9 in _start (/home/fuzz/dp/chunkfuzzer-evaluation/benchmark/gpac-
asan/bin/gcc/MP4Box+0x4e0a9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV scene_manager/scene_dump.c:693 in gf_dump_vrml_sffield
==42376==ABORTING
```

Environment

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

jeanlf closed this as completed in c5249ee on Oct 10

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant