New issue

Jump to bottom

There are memory leaks in the sgpd_parse_entry function of box_code_base.c:9656 #1345

Closed **gutiniao** opened this issue on Nov 13, 2019 · 1 comment

gutiniao commented on Nov 13, 2019

Thanks for reporting your issue. Please make sure these boxes are checked before submitting your issue - thank you!

[√] I looked for a similar issue and couldn't find any.
[√] I tried with the latest version of GPAC. Installers available at http://gpac.io/downloads/gpac-nightly-builds/
[√] I give enough information for contributors to reproduce my issue (meaningful title, github labels, platform and compiler, command-line ...). I can share files anonymously with this dropbox: https://www.mediafire.com/filedrop/filedrop_hosted.php?drop=eec9e058a9486fe4e99c33021481d9e1826ca9dbc242a6cfaab0fe95da5e5d95
Detailed guidelines: http://gpac.io/2013/07/16/how-to-file-a-bug-properly/

A crafted input will lead to crash in box_code_base.c at gpac 0.8.0.

Triggered by
./MP4Box -diso POC -out /dev/null

Poc
007-memleak-sgpd_parse_entry

The ASAN information is as follows:

```
./MP4Box -diso 007-memleak-sgpd_parse_entry -out /dev/null
[iso file] Unknown box type gods in parent moov
[iso file] Box "avcC" (start 939) has 34 extra bytes
[iso file] Unknown box type 0000 in parent sinf
[iso file] Invalid descriptor tag 0xc1 in esds
[iso file] Read Box "esds" (start 1491) failed (Invalid IsoMedia File) - skipping
[iso file] Invalid descriptor tag 0xc1 in esds
[iso file] Read Box "esds" (start 0) failed (Invalid IsoMedia File) - skipping
[isom] not enough bytes in box sgpd: 20 left, reading 63 (file isomedia/box_code_base.c, line 9926)
[iso file] Read Box "sgpd" (start 1678) failed (Invalid IsoMedia File) - skipping
[iso file] Read Box "stbl" (start 1431) failed (Invalid IsoMedia File) - skipping
[iso file] Read Box "minf" (start 1371) failed (Invalid IsoMedia File) - skipping
[iso file] Read Box "mdia" (start 1298) failed (Invalid IsoMedia File) - skipping
[iso file] Read Box "trak" (start 1198) failed (Invalid IsoMedia File) - skipping
[iso file] Read Box "moov" (start 351) failed (Invalid IsoMedia File) - skipping
Error opening file 007-memleak-sgpd_parse_entry: Invalid IsoMedia File

=================================================================
==6751==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 37 byte(s) in 1 object(s) allocated from:
    #0 0x7f25e0370b50 in __interceptor_malloc (/usr/lib/x86_64-linux-gnu/libasan.so.4+0xdeb50)
    #1 0x55e8ff099553 in sgpd_parse_entry isomedia/box_code_base.c:9656
    #2 0x55e8ff099553 in sgpd_Read isomedia/box_code_base.c:9922

SUMMARY: AddressSanitizer: 37 byte(s) leaked in 1 allocation(s)
```

aureliendavid added a commit that referenced this issue on Jan 9, 2020

`add sgpd constant_iv_size check (#1345)` `6c1e7dd`

aureliendavid commented on Jan 9, 2020 Contributor

thanks for the report

this should be fixed by the commit above

reopen if needed

aureliendavid closed this as completed on Jan 9, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants