New issue

Jump to bottom

SEGV in gpac MP4Box function Media_RewriteODFrame #1772

Closed JsHuang opened this issue on Apr 30, 2021 · 1 comment

JsHuang commented on Apr 30, 2021

A SEGV issue was found in MP4Box, to reproduce, compile gpac as follows:

```
CC=gcc CXX=g++ CFLAGS="-fsanitize=address" CXXFLAGS="-fsanitize=address" LDFLAGS="-fsanitize=address" ./configure --enable-debug
```

run poc file :

```
./bin/gcc/MP4Box -hint poc -out /dev/null
```

Detailed ASAN result is as below:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==29303==ERROR: AddressSanitizer: SEGV on unknown address 0x602000021b70 (pc 0x7fc90a84caa9 bp 0x7ffee2653e40 sp 0x7ffee2653da0 T0)
==29303==The signal is caused by a READ memory access.
    #0 0x7fc90a84caa8 in Media_RewriteODFrame isomedia/media_odf.c:135
    #1 0x7fc90a84b02e in Media_GetSample isomedia/media.c:636
    #2 0x7fc90a821813 in gf_isom_get_sample_ex isomedia/isom_read.c:1823
    #3 0x7fc90a8218f3 in gf_isom_get_sample isomedia/isom_read.c:1843
    #4 0x562b406cfc50 in HintFile /home/src/gpac/applications/mp4box/main.c:3412
    #5 0x562b406dae70 in mp4boxMain /home/src/gpac/applications/mp4box/main.c:6209
    #6 0x562b406db653 in main /home/src/gpac/applications/mp4box/main.c:6335
    #7 0x7fc90a3990b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #8 0x562b406c72ad in _start (/home/src/gpac/bin/gcc/MP4Box+0x182ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/media_odf.c:135 in Media_RewriteODFrame
==29303==ABORTING
```

Credit : ADLab of Venustech
poc_segv_media_odf_c_135.zip

jeanlf closed this as completed in `f0ba837` on Apr 30, 2021

jeanlf mentioned this issue on Apr 30, 2021

SEGV in gpac MP4Box in file isom_hinter.c:1271 #1773

Closed

JsHuang commented on Aug 10, 2021 Author

This is CVE-2021-32440

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant