New issue

Jump to bottom

Null pointer dereference in gpac MP4Box gf_media_export_filters #1769

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

JsHuang commented on Apr 30, 2021

A null pointer dereference 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 -nhnt 1 poc -out /dev/null
```

Detailed ASAN result is as below:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2590==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x7f10a4aef7e8 bp 0x7ffc623e3300 sp 0x7ffc623e2c20 T0)
==2590==The signal is caused by a READ memory access.
==2590==Hint: address points to the zero page.
    #0 0x7f10a4aef7e7 in gf_media_export_filters media_tools/media_export.c:1112
    #1 0x7f10a4af1146 in gf_media_export media_tools/media_export.c:1474
    #2 0x5605c1f30d36 in do_export_tracks /home/lab4/src/gpac/applications/mp4box/main.c:4646
    #3 0x5605c1f35f6a in mp4boxMain /home/lab4/src/gpac/applications/mp4box/main.c:5971
    #4 0x5605c1f37653 in main /home/lab4/src/gpac/applications/mp4box/main.c:6335
    #5 0x7f10a455a0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #6 0x5605c1f232ad in _start (/home/lab4/src/gpac/bin/gcc/MP4Box+0x182ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV media_tools/media_export.c:1112 in gf_media_export_filters
==2590==ABORTING
```

Credit : ADLab of Venustech

poc-null.zip

jeanlf closed this as completed in 00194f5 on Apr 30, 2021

JsHuang commented on Aug 10, 2021 Author

This is CVE-2021-32438

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant