Null pointer dereference in function gf_hinter_finalize isom_hinter.c:1236 #1770

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 -hint poc -out /dev/null
```

Detailed ASAN result is as below:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==1042==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7fc3d4e76d0b bp 0x7ffd390b09a0 sp 0x7ffd390ae160 T0)
==1042==The signal is caused by a READ memory access.
==1042==Hint: address points to the zero page.
    #0 0x7fc3d4e76d0a in gf_hinter_finalize media_tools/isom_hinter.c:1236
    #1 0x555a478a9019 in HintFile /home/lab4/src/gpac/applications/mp4box/main.c:3467
    #2 0x555a478b3e70 in mp4boxMain /home/lab4/src/gpac/applications/mp4box/main.c:6209
    #3 0x555a478b4653 in main /home/lab4/src/gpac/applications/mp4box/main.c:6335
    #4 0x7fc3d48bc0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #5 0x555a478a02ad in _start (/home/lab4/src/gpac/bin/gcc/MP4Box+0x182ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV media_tools/isom_hinter.c:1236 in gf_hinter_finalize
==1042==ABORTING
```

Credit : ADLab of Venustech
poc_null.zip

jeanlf closed this as completed in 1653f31 on Apr 30, 2021

JsHuang commented on Aug 10, 2021 Author

This is CVE-2021-32437

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant