New issue

Jump to bottom

null dereference in MP4Box HintFile #1734

Closed **5n1p3r0010** opened this issue on Apr 8, 2021 · 0 comments

5n1p3r0010 commented on Apr 8, 2021

Hi,

There is a null dereference issue with gpac MP4Box,this can reproduce on the lattest commit.

Steps To Reproduce

build:

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

run as:

```
MP4Box -hint <poc> -out /dev/null
```

shows the following log:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==846752==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x56258571da70 bp 0x7ffd80134400 sp 0x7ffd80134330 T0)
==846752==The signal is caused by a READ memory access.
==846752==Hint: address points to the zero page.
    #0 0x56258571da6f in HintFile /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3374
    #1 0x562585728d7c in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6186
    #2 0x56258572954d in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6312
    #3 0x7f29df2d30b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #4 0x56258571520d in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x1820d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:3374 in HintFile
==846752==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
null.zip

jeanlf closed this as completed in 87afe07 on Apr 8, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant