

New issue

Jump to bottom

[Security]stack overflow(oob) in MP4Box #1780

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

5n1p3r0010 commented on May 8, 2021

Hi,

There is a stack overflow(oob) issue in gpac MP4Box hevc_parse_vps_extension,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 --enable-debug
make
```

run as:

```
MP4Box -info <poc>
```

shows the following log:


```
=====
==2453140==ERROR: AddressSanitizer: stack-overflow on address 0x7ffc877550e9 (pc 0x7f477fb886b3 bp 0x7ffc87747b40 sp 0x7ffc87747870 T0)
#0 0x7f477fb886b2 in hevc_parse_vps_extension media_tools/av_parsers.c:7514
#1 0x7f477fb89ae3 in gf_hevc_read_vps_bs_internal media_tools/av_parsers.c:7745
#2 0x7f477fb8ce3a in gf_hevc_parse_nalu_bs media_tools/av_parsers.c:8373
#3 0x7f477ff46cf9 in naludmx_parse_nal_hevc filters/reframe_nalu.c:1997
#4 0x7f477ff49a41 in naludmx_process_filters/reframe_nalu.c:2864
#5 0x7f477fdd631f in gf_filter_process_task filter_core/filter.c:2405
#6 0x7f477fdc59b8 in gf_fs_thread_proc filter_core/filter_session.c:1610
#7 0x7f477fdc633f in gf_fs_run filter_core/filter_session.c:1847
#8 0x7f477fb9fa91 in gf_media_import media_tools/media_import.c:1173
#9 0x55905a1a7a44 in convert_file_info /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/fileimport.c:128
#10 0x55905a19226e in mp4boxMain /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:5804
#11 0x55905a194653 in main /home/r00t/fuzz/target/tmp/gpac/applications/mp4box/main.c:6333
#12 0x7f477f6400b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
#13 0x55905a1802ad in _start (/home/r00t/fuzz/target/tmp/gpac/bin/gcc/MP4Box+0x182ad)

SUMMARY: AddressSanitizer: stack-overflow media_tools/av_parsers.c:7514 in hevc_parse_vps_extension
==2453140==ABORTING
```

Reporter:

5n1p3r0010 from Topsec Alpha Lab
[stack-overflow_hevc_parse_vps_extension.zip](#)

 jeanlf closed this as completed in 1273cdc on May 10, 2021

 jeanlf mentioned this issue on May 10, 2021

oob in MP4Box #1781

 Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

