New issue

Jump to bottom

Out of bounds Write in stbl_write.c:1650 #1774

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

JsHuang commented on Apr 30, 2021

A OOB Write 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:

```
15305==ERROR: AddressSanitizer: SEGV on unknown address 0x616000010000 (pc 0x7ff3a3276461 bp 0x7ffc231be4c0 sp 0x7ffc231be490 T0)
==15305==The signal is caused by a WRITE memory access.
    #0 0x7ff3a3276460 in stbl_AppendSize isomedia/stbl_write.c:1650
    #1 0x7ff3a3279df4 in MergeTrack isomedia/track.c:703
    #2 0x7ff3a3225f85 in MergeFragment isomedia/isom_intern.c:90
    #3 0x7ff3a3227ec2 in gf_isom_parse_movie_boxes_internal isomedia/isom_intern.c:649
    #4 0x7ff3a3228488 in gf_isom_parse_movie_boxes isomedia/isom_intern.c:777
    #5 0x7ff3a322881b in gf_isom_open_file isomedia/isom_intern.c:897
    #6 0x7ff3a322b7f7 in gf_isom_open isomedia/isom_read.c:520
    #7 0x558e07ad4e7e in mp4boxMain /home/src/gpac/applications/mp4box/main.c:5722
    #8 0x558e07ad7653 in main /home/src/gpac/applications/mp4box/main.c:6335
    #9 0x7ff3a2da60b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #10 0x558e07ac32ad in _start (/home/src/gpac/bin/gcc/MP4Box+0x182ad)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV isomedia/stbl_write.c:1650 in stbl_AppendSize
==15305==ABORTING
```

Credit : ADLab of Venustech
oob_write_stbl_write_c_1650.zip

jeanlf closed this as completed in 77ed81c on Apr 30, 2021

JsHuang commented on Aug 10, 2021 Author

This is CVE-2021-32439

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant