New issue

Jump to bottom

From mp4fragment: SEGV on unknown address 0x000000000000 #767

Open DylanSec opened this issue on Sep 21 · 0 comments

DylanSec commented on Sep 21 • edited

Summary

Hi there, I use my fuzzer for fuzzing the binary mp4fragment, the version of Bento4 is the latest (the newest master branch) and the operation system is Ubuntu 18.04.6 LTS (docker) and this binary crashes with the following.

Details

```
root@4e3b7f9edc0d:/mp4box/mp4fragment# ./mp4fragment
../out/crashes/id\:000000\,sig\:06\,src\:000008\,op\:flip1\,pos\:31325\,4970731 /dev/null
unable to autodetect fragment duration, using default
AddressSanitizer:DEADLYSIGNAL
=================================================================
==750986==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f5fc13c0306 bp
0x7ffe16f62f30 sp 0x7ffe16f626c8 T0)
==750986==The signal is caused by a READ memory access.
==750986==Hint: address points to the zero page.
    #0 0x7f5fc13c0306  (/lib/x86_64-linux-gnu/libc.so.6+0xb1306)
    #1 0x94da2c in __interceptor_strlen.part.36 /llvm-project/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:370
    #2 0x6ec0c2 in AP4_TrakAtom::AP4_TrakAtom(AP4_SampleTable*, unsigned int, char const*,
unsigned int, unsigned long long, unsigned long long, unsigned long long, unsigned int, unsigned
long long, unsigned short, char const*, unsigned int, unsigned int, unsigned short, unsigned
short, int const*) (/mp4box/mp4fragment/mp4fragment+0x6ec0c2)
    #3 0x432bbc in main (/mp4box/mp4fragment/mp4fragment+0x432bbc)
    #4 0x7f5fc1330c86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #5 0x407cd9 in _start (/mp4box/mp4fragment/mp4fragment+0x407cd9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0xb1306)
```

```
==750986==ABORTING
```

POC

POC-Mp4fragment-1.zip

Environment

Ubuntu 18.04.6 LTS (docker)
clang 12.0.1
clang++ 12.0.1
Bento4 master branch(`5b7cc25`) && Bento4 release version(1.6.0-639)

Credit

Xudong Cao (NCNIPC of China)
Jiayuan Zhang (NCNIPC of China)
Han Zheng (NCNIPC of China, Hexhive)

Thank you for your time!

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant