axiomatic-systems / **Bento4** Public

Code · Issues 422 · Pull requests 28 · Actions · Projects · Wiki · ...

New issue

Jump to bottom

SEGV in mp42aac #616

Open · **dhbbb** opened this issue on Jun 10, 2021 · 1 comment

Labels fuzzing

dhbbb commented on Jun 10, 2021

Hello,
A SEGV has occurred when running program mp42aac,
System info:
Ubuntu 20.04.1 : clang 10.0.0 , gcc 9.3.0

Bento4 version 1.6.0-636

poc (2).zip

Verification steps:
1.Get the source code of Bento4
2.Compile

```
cd Bento4
mkdir check_build && cd check_build
cmake ../ -DCMAKE_CXX_COMPILER=clang++ -DCMAKE_CXX_FLAGS="fsanitize=address"
make -j 16
```

3.run mp42aac

```
./mp42aac poc /dev/null
```

Output

```
Segmentation fault(core dumped)
```

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2513287==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x5614212cf0c2 bp 0x0fffb285532c sp 0x7ffd942a9960 T0)
==2513287==The signal is caused by a READ memory access.
==2513287==Hint: address points to the zero page.
    #0 0x5614212cf0c1 in AP4_DescriptorFinder::Test(AP4_Descriptor*) const /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Descriptor.h:92
    #1 0x5614212cf0c1 in AP4_List<AP4_Descriptor>::Find(AP4_List<AP4_Descriptor>::Item::Finder const&, AP4_Descriptor*&) const /home/dh/AFLplusplus/Bento4-master/Bento4-master-
afl++/Source/C++/Core/Ap4List.h:431
    #2 0x5614212cf0c1 in AP4_DecoderConfigDescriptor::GetDecoderSpecificInfoDescriptor() const /home/dh/AFLplusplus/Bento4-master/Bento4-master-
afl++/Source/C++/Core/Ap4DecoderConfigDescriptor.cpp:159
    #3 0x5614211be076 in AP4_MpegSampleDescription::AP4_MpegSampleDescription(unsigned int, AP4_EsdsAtom*) /home/dh/AFLplusplus/Bento4-master/Bento4-master-
afl++/Source/C++/Core/Ap4SampleDescription.cpp:894
    #4 0x5614211be5e5 in AP4_MpegAudioSampleDescription::AP4_MpegAudioSampleDescription(unsigned int, unsigned short, unsigned short, AP4_EsdsAtom*) /home/dh/AFLplusplus/Bento4-
master/Bento4-master-afl++/Source/C++/Core/Ap4SampleDescription.cpp:1000
    #5 0x561421193a74 in AP4_EncaSampleEntry::ToTargetSampleDescription(unsigned int) /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Protection.cpp:143
    #6 0x5614211a1105 in AP4_EncaSampleEntry::ToSampleDescription() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Protection.cpp:98
    #7 0x5614211dfd8d in AP4_StsdAtom::GetSampleDescription(unsigned int) /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4StsdAtom.cpp:181
    #8 0x561421175063 in main /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:268
    #9 0x7fcdb4b710b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #10 0x56142117914d in _start (/home/dh/sda3/AFLplusplus/Bento4-master/mp42aac_afl+++0x5914d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Descriptor.h:92 in AP4_DescriptorFinder::Test(AP4_Descriptor*) const
==2513287==ABORTING
```

barbibulle added the **fuzzing** label on Jul 22, 2021

dhbbb commented on Aug 5, 2021 Author

This is CVE-2021-35307

Assignees

No one assigned

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants