New issue

Jump to bottom

SEGV in mp42aac #615

Open dhbbb opened this issue on Jun 10, 2021 · 2 comments

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.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
=================================================================
==2182861==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x556efda097b2 bp 0x6040000008d0 sp 0x7ffc29113390 T0)
==2182861==The signal is caused by a READ memory access.
==2182861==Hint: address points to the zero page.
    #0 0x556efda097b1 in AP4_StszAtom::WriteFields(AP4_ByteStream&) /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4StszAtom.cpp:122
    #1 0x556efd8c3e32 in AP4_Atom::Write(AP4_ByteStream&) /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Atom.cpp:229
    #2 0x556efd8c2bea in AP4_Atom::Clone() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Atom.cpp:316
    #3 0x556efd9306b7 in AP4_ContainerAtom::Clone() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4ContainerAtom.cpp:172
    #4 0x556efd9306b7 in AP4_ContainerAtom::Clone() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4ContainerAtom.cpp:172
    #5 0x556efd9306b7 in AP4_ContainerAtom::Clone() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4ContainerAtom.cpp:172
    #6 0x556efd9306b7 in AP4_ContainerAtom::Clone() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4ContainerAtom.cpp:172
    #7 0x556efd9306b7 in AP4_ContainerAtom::Clone() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4ContainerAtom.cpp:172
    #8 0x556efd82dc02 in AP4_ProtectionSchemeInfo::AP4_ProtectionSchemeInfo(AP4_ContainerAtom*) /home/dh/AFLplusplus/Bento4-master/Bento4-master-
afl++/Source/C++/Core/Ap4Protection.cpp:319
    #9 0x556efd82dc02 in AP4_ProtectedSampleDescription::AP4_ProtectedSampleDescription(unsigned int, AP4_SampleDescription*, unsigned int, unsigned int, unsigned int, char const*,
AP4_ContainerAtom*, bool) /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Protection.cpp:689
    #10 0x556efd82e1f5 in AP4_EncaSampleEntry::ToSampleDescription() /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4Protection.cpp:103
    #11 0x556efd86cd8d in AP4_StsdAtom::GetSampleDescription(unsigned int) /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Core/Ap4StsdAtom.cpp:181
    #12 0x556efd802063 in main /home/dh/AFLplusplus/Bento4-master/Bento4-master-afl++/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:268
    #13 0x7f76227050b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2)
    #14 0x556efd80614d 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/Ap4StszAtom.cpp:122 in AP4_StszAtom::WriteFields(AP4_ByteStream&)
==2182861==ABORTING
```

barbibulle added the fuzzing label on Jul 22, 2021

dhbbb commented on Aug 5, 2021 Author

This is CVE-2021-35306

0xdd96 commented on Dec 27, 2021

I cannot reproduce your crash in Bento4 version 1.6.0-636, but SUCCEEDED in Bento4 version 1.6.0-637. Is the version number you provided wrong?

Assignees

No one assigned

Labels

fuzzing

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants