New issue

Jump to bottom

Bad-free with ASAN in mp42aac #765

Open **17ssDP** opened this issue on Sep 19 · 0 comments

17ssDP commented on Sep 19

Hi, developers of Bento4:
In the test of the binary mp42aac instrumented with ASAN. There are some inputs causing attempting free on address which was not malloc. Here is the ASAN mode output:

==9252==ERROR: AddressSanitizer: attempting free on address which was not malloc()-ed: 0x60200000ef50 in thread T0
#0 0x7ffff6f03d0a in operator delete (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99d0a)
#1 0x5c124b in AP4_HdlrAtom::~AP4_HdlrAtom() /root/Bento4/Source/C++/Core/Ap4HdlrAtom.h:61
#2 0x5c124b in AP4_HdlrAtom::~AP4_HdlrAtom() /root/Bento4/Source/C++/Core/Ap4HdlrAtom.h:61
#3 0x4e7e4b in AP4_List<AP4_Atom>::DeleteReferences() /root/Bento4/Source/C++/Core/Ap4List.h:476
#4 0x4e7e4b in AP4_AtomParent::~AP4_AtomParent() /root/Bento4/Source/C++/Core/Ap4Atom.cpp:516
#5 0x57a323 in AP4_ContainerAtom::~AP4_ContainerAtom()
/root/Bento4/Source/C++/Core/Ap4ContainerAtom.h:48
#6 0x57a323 in AP4_ContainerAtom::~AP4_ContainerAtom()
/root/Bento4/Source/C++/Core/Ap4ContainerAtom.h:48
#7 0x4e7e4b in AP4_List<AP4_Atom>::DeleteReferences() /root/Bento4/Source/C++/Core/Ap4List.h:476
#8 0x4e7e4b in AP4_AtomParent::~AP4_AtomParent() /root/Bento4/Source/C++/Core/Ap4Atom.cpp:516
#9 0x417b8d in AP4_File::~AP4_File() /root/Bento4/Source/C++/Core/Ap4File.cpp:84
#10 0x417b8d in AP4_File::~AP4_File() /root/Bento4/Source/C++/Core/Ap4File.cpp:88
#11 0x4043f2 in main /root/Bento4/Source/C++/Apps/Mp42Aac/Mp42Aac.cpp:303
#12 0x7ffff61bb83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
#13 0x408508 in _start (/root/Bento4/mp42aac+0x408508)

0x60200000ef50 is located 0 bytes inside of 1-byte region [0x60200000ef50,0x60200000ef51)
allocated by thread T0 here:
#0 0x7ffff6f03712 in operator new[](unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99712)
#1 0x48ac75 in AP4_String::Assign(char const*, unsigned int)
/root/Bento4/Source/C++/Core/Ap4String.cpp:165
#2 0x48ac75 in AP4_String::operator=(char const*) /root/Bento4/Source/C++/Core/Ap4String.cpp:123

SUMMARY: AddressSanitizer: bad-free ??:0 operator delete
==9252==ABORTING

Crash input

https://github.com/17ssDP/fuzzer_crashes/blob/main/Bento4/mp42aac-badfree

Validation steps

git clone https://github.com/axiomatic-systems/Bento4
cd Bento4/
mkdir check_build && cd check_build
cmake ../ -DCMAKE_C_COMPILER=clang -DCMAKE_CXX_COMPILER=clang++ -DCMAKE_C_FLAGS="-fsanitize=address" -DCMAKE_CXX_FLAGS="-fsanitize=address" -DCMAKE_BUILD_TYPE=Release
make -j
./mp42aac mp42aac-badfree /dev/null

Environment

Ubuntu 16.04
Clang 10.0.1
gcc 5.5

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant