New issue

Jump to bottom

Segmentation fault caused by null pointer dereference in MP4fragment, Ap4StsdAtom.cpp:75 #800

Open **5hadowblad3** opened this issue on Oct 19 · 0 comments

5hadowblad3 commented on Oct 19

Hi, there.

There is a segmentation fault caused by null pointer dereference in MP4fragment, Ap4StsdAtom.cpp:75 in the newest commit `5e7bb34` .

The reason for this issue is that the return value of the GetSampleDescription is unchecked.

```
52 +---------------------------------------------------------------------*/
53 AP4_StsdAtom::AP4_StsdAtom(AP4_SampleTable* sample_table) :
54     AP4_ContainerAtom(AP4_ATOM_TYPE_STSD, (AP4_UI32)0, (AP4_UI32)0)
55 {
56     m_Size32 += 4;
57     AP4_Cardinal sample_description_count = sample_table->GetSampleDescriptionCount();
58     m_SampleDescriptions.EnsureCapacity(sample_description_count);
59     for (AP4_Ordinal i=0; i<sample_description_count; i++) {
70         // clear the cache entry
71         m_SampleDescriptions.Append(NULL);
72
                                    null pointer could be returned at Line 74 without checking
73         // create an entry for the description
74         AP4_SampleDescription* sample_description = sample_table->GetSampleDescription(i);
75         AP4_Atom* entry = sample_description->ToAtom();
76         AddChild(entry);
77     }
```

To reproduce, run:

```
./mp4fragment poc /dev/null
```

Here is the trace reported by ASAN:

```
==3437252==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000005fcb24 bp
0x60b000000300 sp 0x7ffec2967f00 T0)
 ==3437252==The signal is caused by a READ memory access.
 ==3437252==Hint: address points to the zero page.
     #0 0x5fcb24 in AP4_StsdAtom::AP4_StsdAtom(AP4_SampleTable*)
```

```
/benchmark/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:75:47
    #1 0x6b7b51 in AP4_SampleTable::GenerateStblAtom(AP4_ContainerAtom*&)
/benchmark/Bento4/Source/C++/Core/Ap4SampleTable.cpp:59:30
    #2 0x620f26 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*)  /benchmark/Bento4/Source/C++/Core/Ap4TrakAtom.cpp:131:28
    #3 0x61e255 in AP4_Track::AP4_Track(AP4_SampleTable*, unsigned int, unsigned int, unsigned
long long, unsigned int, unsigned long long, AP4_Track const*)
/benchmark/Bento4/Source/C++/Core/Ap4Track.cpp:183:22
    #4 0x500733 in Fragment(AP4_File&, AP4_ByteStream&, AP4_Array<TrackCursor*>&, unsigned int,
unsigned int, bool, bool, bool)
/benchmark/Bento4/Source/C++/Apps/Mp4Fragment/Mp4Fragment.cpp:360:39
    #5 0x500733 in main  /benchmark/Bento4/Source/C++/Apps/Mp4Fragment/Mp4Fragment.cpp:1475:5
    #6 0x7f0f643e9082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #7 0x41d8ad in _start ( /benchmark/Bento4/build-a/mp4fragment+0x41d8ad)

 AddressSanitizer can not provide additional info.
 SUMMARY: AddressSanitizer: SEGV  /benchmark/Bento4/Source/C++/Core/Ap4StsdAtom.cpp:75:47 in
AP4_StsdAtom::AP4_StsdAtom(AP4_SampleTable*)
 ==3437252==ABORTING
```

mp4fragment_npd_Ap4StsdAtom.cpp75.zip
(unzip first)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant