New issue

Jump to bottom

Divide-by-zero in AC3Codec::decodeDtsHdFrame #428

Closed **cemonatk** opened this issue on May 24, 2021 · 0 comments

Labels bug

cemonatk commented on May 24, 2021 • edited

Hi, please see asan output and poc file below.

Found by **Cem Onat Karagun of Diesec**.

System info:

```
Ubuntu 21.04
tsMuxeR version git-f6ab2a2
```

To run PoC after unzip:

```
$ ./tsmuxer decoder_poc
```

decoder_poc.zip

References:

https://cwe.mitre.org/data/definitions/369.html

ASAN output:

```
tsMuxeR version git-f6ab2a2. github.com/justdan96/tsMuxer
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2890753==ERROR: AddressSanitizer: FPE on unknown address 0x000000444db8 (pc 0x000000444db8 bp 0x7ffd085984a0 sp 0x7ffd085983a0 T0)
    #0 0x444db8 in AC3Codec::decodeDtsHdFrame(unsigned char*, unsigned char*) /src/build/../tsMuxer/ac3Codec.cpp:377:65
    #1 0x4478d9 in AC3Codec::decodeFrame(unsigned char*, unsigned char*, int&) /src/build/../tsMuxer/ac3Codec.cpp:428:34
    #2 0x7c61df in SimplePacketizerReader::checkStream(unsigned char*, int, AbstractStreamReader::ContainerType, int, int) /src/build/../tsMuxer/simplePacketizerReader.cpp:257:13
    #3 0x6cf93a in METADemuxer::detectTrackReader(unsigned char*, int, AbstractStreamReader::ContainerType, int, int) /src/build/../tsMuxer/metaDemuxer.cpp:755:20
    #4 0x6c7255 in METADemuxer::DetectStreamReader(BufferedReaderManager&, std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> > const&, bool)
/src/build/../tsMuxer/metaDemuxer.cpp:684:35
    #5 0x5df87e in detectStreamReader(char const*, MPLSParser*, bool) /src/build/../tsMuxer/main.cpp:120:34
    #6 0x5efd05 in main /src/build/../tsMuxer/main.cpp:698:17
    #7 0x7f2c99a1a564 in __libc_start_main csu/../csu/libc-start.c:332:16
    #8 0x2ebded in _start (/home/Fuzzer_Instance_29/txmux/tsMuxer/bin/tsMuxeR+0x2ebded)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /src/build/../tsMuxer/ac3Codec.cpp:377:65 in AC3Codec::decodeDtsHdFrame(unsigned char*, unsigned char*)
==2890753==ABORTING
```

jcdr428 mentioned this issue on May 24, 2021

[bug] Division by 0 #421

Merged

cemonatk changed the title ~~Denial of Service in AC3Codec::decodeDtsHdFrame~~ Divide-by-zero in AC3Codec::decodeDtsHdFrame on May 24, 2021

xavery pushed a commit that referenced this issue on Jun 9, 2021

`[bug] Division by 0 (#421)` ... ✓ 9070a99

xavery closed this as completed on Jun 9, 2021

jcdr428 added the bug label on Jun 23

Assignees

No one assigned

Labels

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants