#9651 closed defect (fixed)

Opened 9 months ago
Closed 9 months ago

Assertion next >= 0 || pc->buffer failed at libavcodec/parser.c:240

Reported by:	andreafioraldi	Owned by:	
Priority:	normal	Component:	avcodec
Version:	unspecified	Keywords:	
Cc:		Blocked By:	
Blocking:		Reproduced by developer:	no
Analyzed by developer:	no		

Description (last modified by andreafioraldi) Δ

This bug was found by fuzzing the current master branch, to reproduce it you have to build the OSS-Fuzz harness for FFmpeg with ASan and UBsan.

You can use the scripts in https://github.com/google/oss-fuzz/tree/master/projects/ffmpeg with clang as compiler and the following flags:

```
CFLAGS='-O1 -fsanitize=address -fsanitize=array-bounds,bool,builtin,enum,float-
CXXFLAGS='-O1 -fsanitize=address -fsanitize=array-bounds,bool,builtin,enum,floa
```

The sanitizer report when executing the testcase is the following:

```
INFO: Seed: 108531316
INFO: Loaded 1 modules   (436082 inline 8-bit counters): 436082 [0x2f32583, 0x2
INFO: Loaded 1 PC tables (436082 PCs): 436082 [0x1d0bf68,0x23b3688),
/out/ffmpeg_DEMUXER_fuzzer: Running 1 inputs 1 time(s) each.
Running: crashes/ffmpeg_ffmpeg_demuxer_fuzzer/id:000169,sig:06,src:012185,time:
libavcodec/g729_parser.c:51:23: runtime error: signed integer overflow: 10 * 80
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libavcodec/g729_parser.
Assertion next >= 0 || pc->buffer failed at libavcodec/parser.c:240
==1324766== ERROR: libFuzzer: deadly signal
    #0 0x4a20f1 in __sanitizer_print_stack_trace (/out/ffmpeg_DEMUXER_fuzzer+0x
    #1 0x19f3828 in fuzzer::PrintStackTrace() (/out/ffmpeg_DEMUXER_fuzzer+0x19f
    #2 0x19d8629 in fuzzer::Fuzzer::CrashCallback() (/out/ffmpeg_DEMUXER_fuzzer
    #3 0x7ffff7e033bf  (/lib/x86_64-linux-gnu/libpthread.so.0+0x153bf)
    #4 0x7ffff7a3218a in __libc_signal_restore_set /build/glibc-eX1tMB/glibc-2.
    #5 0x7ffff7a3218a in raise /build/glibc-eX1tMB/glibc-2.31/signal/../sysdeps
    #6 0x7ffff7a11858 in abort /build/glibc-eX1tMB/glibc-2.31/stdlib/abort.c:79
    #7 0xa628d2 in ff_combine_frame /src/ffmpeg/libavcodec/parser.c:240:5
    #8 0xc9ca5f in g729_parse /src/ffmpeg/libavcodec/g729_parser.c:71:9
    #9 0xa5fdd3 in av_parser_parse2 /src/ffmpeg/libavcodec/parser.c:164:13
    #10 0x502cca in parse_packet /src/ffmpeg/libavformat/demux.c:1126:15
    #11 0x4e8013 in read_frame_internal /src/ffmpeg/libavformat/demux.c:1240:21
    #12 0x4f343c in avformat_find_stream_info /src/ffmpeg/libavformat/demux.c:2
    #13 0x4cba3e in LLVMFuzzerTestOneInput /src/ffmpeg/tools/target_dem_fuzzer.
    #14 0x19d9d59 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsi
    #15 0x19c4c69 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned
    #16 0x19c9b72 in fuzzer::FuzzerDriver(int*, char***, int (*)(unsigned char
    #17 0x19c49f2 in main (/out/ffmpeg_DEMUXER_fuzzer+0x19c49f2)
    #18 0x7ffff7a130b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/
    #19 0x420e7d in _start (/out/ffmpeg_DEMUXER_fuzzer+0x420e7d)

NOTE: libFuzzer has rudimentary signal handlers
```

```
NOTE: libFuzzer has rudimentary signal handlers.
      Combine libFuzzer with AddressSanitizer or similar for better crash repor
SUMMARY: libFuzzer: deadly signal
```

There is an UBSan violation that is likely the root cause of the failed assertion.
You find the crashing testcase attached, execute it with `./ffmpeg_DEMUXER_fuzzer ./testcase`

Attachments (1)

- id:000169,sig:06,src:012185,time:73697278,op:havoc,rep:4,trial:1493913 (311 bytes) - added by andreafioraldi 9 months ago.
  the crashing testcase

Change History (3)

by andreafioraldi, 9 months ago

Attachment: *id:000169,sig:06,src:012185,time:73697278,op:havoc,rep:4,trial:1493913* added

the crashing testcase

comment:1 by andreafioraldi, 9 months ago

Description: modified (diff)

comment:2 by Balling, 9 months ago

Resolution: → fixed
Status: new → closed

Fixed in 757da974b21833529cc41bdcc9684c29660cdfa8.

Note: See TracTickets for help on using tickets.