New issue

Jump to bottom

bugs found #54

Closed **Cvjark** opened this issue on Aug 4 · 1 comment

Cvjark commented on Aug 4

Hi, in the lastest version of this repo [PS: commit ID -> `1a1ee29`], I found something insterest.

POC

1id0-heap-buffer-overflow.zip

command to reproduce

```
./fdkaac -p5 -b64 POC -o /dev/null
```

output

```
==122363==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x625000018900 at pc
0x00000043b985 bp 0x7ffe69d827d0 sp 0x7ffe69d81f80
READ of size 4 at 0x625000018900 thread T0
    #0 0x43b984 in __interceptor_memcpy.part.46 /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:810
    #1 0x7fe7e606c24a in aacEncEncode (/usr/lib/x86_64-linux-gnu/libfdk-aac.so.1+0x2424a)
    #2 0x4f7154 in aac_encode_frame /home/bupt/Desktop/fdkaac/src/aacenc.c:291:11
    #3 0x51fd71 in encode /home/bupt/Desktop/fdkaac/src/main.c:554:24
    #4 0x51fd71 in main /home/bupt/Desktop/fdkaac/src/main.c:862:19
    #5 0x7fe7e5097c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #6 0x41c9d9 in _start (/home/bupt/Desktop/fdkaac/fdkaac+0x41c9d9)

0x625000018900 is located 0 bytes to the right of 8192-byte region [0x625000016900,0x625000018900)
allocated by thread T0 here:
    #0 0x4aefa0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x51fb60 in encode /home/bupt/Desktop/fdkaac/src/main.c:535:12
    #2 0x51fb60 in main /home/bupt/Desktop/fdkaac/src/main.c:862:19
    #3 0x7fe7e5097c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:810 in
__interceptor_memcpy.part.46
Shadow bytes around the buggy address:
  0x0c4a7fffb0d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fffb0e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fffb0f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fffb100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c4a7fffb110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c4a7fffb120:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fffb130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fffb140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fffb150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fffb160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c4a7fffb170: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==122363==ABORTING
```

POC

3id0-FPE.zip

command to reproduce

```
./fdkaac -p5 -b64 POC -o /dev/null
```

output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==122379==ERROR: AddressSanitizer: FPE on unknown address 0x00000053ade9 (pc 0x00000053ade9 bp
0x7ffe2be4ff90 sp 0x7ffe2be4fc60 T0)
    #0 0x53ade9 in wav_open /home/bupt/Desktop/fdkaac/src/wav_reader.c:212:54
    #1 0x51e35b in open_input /home/bupt/Desktop/fdkaac/src/main.c:746:27
    #2 0x51e35b in main /home/bupt/Desktop/fdkaac/src/main.c:802:19
    #3 0x7f17fe499c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #4 0x41c9d9 in _start (/home/bupt/Desktop/fdkaac/fdkaac+0x41c9d9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: FPE /home/bupt/Desktop/fdkaac/src/wav_reader.c:212:54 in wav_open
==122379==ABORTING
```

 **nu774** closed this as completed in `ecddb7d` on Aug 4

---

nu774 added a commit that referenced this issue on Aug 4

 `extrapolater: don't return more samples than required` ... `0ce71d0`

nu774 commented on Aug 4 — Owner

Thanks, fixed on v1.0.4

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants