Opened 3 months ago
Last modified 3 months ago

#2404 new defect

A heap-buffer-overflow occurred in function play() of libaf/af_pan.c

Reported by:	ylzs	Owned by:	beastd
Priority:	normal	Component:	undetermined
Version:	HEAD	Severity:	major
Keywords:		Cc:	
Blocked By:		Blocking:	
Reproduced by developer:	no	Analyzed by developer:	no

Description (last modified by ylzs) ∆

Version: SVN-r38374-13.0.1

Build command: ../configure --disable-ffmpeg_a && make (compiling with asan)

Summary of the bug: An heap-buffer-overflow is found in fucnction play() which affects mencoder. and mplayer The attached file can reproduce this issue (ASAN-recompilation is needed).

How to reproduce:
1.Command: ./mencoder -ovc lavc -oac lavc -o /dev/null ./testcase
./mplayer ./testcase

2.Result:

```
=================================================================
==27905==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6140000003c
READ of size 4 at 0x6140000003c8 thread T0
    #0 0x5555557f69f4 in play /home/jlx/good_mplayer/mplayer/libaf/af_pan.c:176

0x6140000003cb is located 0 bytes to the right of 395-byte region [0x6140000002
allocated by thread T0 here:
    #0 0x5555556fa43d in malloc (/home/jlx/good_mplayer/asan_mplayer/mencoder+0
    #1 0x5555557c795b in af_resize_local_buffer /home/jlx/good_mplayer/mplayer/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/jlx/good_mplayer/mplayer/
Shadow bytes around the buggy address:
  0x0c287fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c287fff8030: 00 00 00 00 00 00 00 00 00 06 fa fa fa fa fa fa
  0x0c287fff8040: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c287fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c287fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c287fff8070: 00 00 00 00 00 00 00 00 00[03]fa fa fa fa fa fa
  0x0c287fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

  0x0c287fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c287fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c287fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c287fff80c0: 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
==27905==ABORTING
```

Attachments (2)

- testcase (3.7 KB) - added by ylzs 3 months ago.
- valgrind (17.9 KB) - added by ylzs 3 months ago.

Change History (7)

by ylzs, 3 months ago

Attachment: *testcase* added

comment:1 by reimar, 3 months ago

Title seems incorrect as this seems to be in af_pan.c, too.
I also expect this to be a duplicate of #2400, though I currently cannot reproduce either.

comment:2 by ylzs, 3 months ago

yes, It seems as same as the 2400.

comment:3 by ylzs, 3 months ago

Description: modified (diff)

Summary: A heap-buffer-overflow occurred in function play() of libaf/af.c:639 → A heap-buffer-overflow occurred in function play() of libaf/af_pan.c

I 've ran this testcase with valgrind and put the valgrind output into the attached file. It is strange that valgrind doesn't report this bug but asan does show that the bug exists.

by ylzs, 3 months ago

Attachment: *valgrind* added

comment:4 by reimar, 3 months ago

I can imagine something goes wrong in af_pan with high channel counts, so don't take this as me denying there is a bug.
But I cannot reproduce it with valgrind or asan, and you can't reproduce it with valgrind, and by the information in another ticket you seem to be running a pre-release version of clang, so maybe it's actually your ASAN/compiler that is buggy?
Anyway at the moment I don't see much I can do about this issue.

comment:5 by ylzs, 3 months ago

I absolutely agree with you and I think the #2400 and #2404 maybe the same cases.

Note: See TracTickets for help on using tickets.