Starred by 7 users

Owner: huisu@google.com
Last visit > 30 days ago

CC: huisu@google.com

Status: Fixed *(Closed)*

Components: ----

Modified: Apr 9, 2021

Type-Defect
Priority-Medium
Hotlist-AOM-OKR

Issue 2911: stack-buffer-overflow in stats/rate_hist.c:185
Reported by zodf0...@gmail.com on Wed, Dec 23, 2020, 11:10 PM EST

What steps will reproduce the problem?
1. ./aomenc --pass=2 --q-hist=5 --usage=1 -o /dev/null poc2

What is the expected output?

This is ASAN report:
```
➜ Yuan-fuzz /home/yuan/afl-target/aom/build/aomenc --pass=2 --q-hist=5 --usage=1 -o /dev/null poc2
Warning: Assuming --pass=2 implies --passes=2

Warning: Enforcing one-pass encoding in realtime mode

Warning: non-zero lag-in-frames option ignored in realtime mode.


Quantizer Selection:
==================================================================
==7890==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffce729bd78 at pc 0x55dcda90736a bp 0x7ffce729bca0 sp 0x7ffce729bc90
READ of size 4 at 0x7ffce729bd78 thread T0
    #0 0x55dcda907369 in show_histogram /home/yuan/afl-target/aom/stats/rate_hist.c:185
    #1 0x55dcda908fb4 in show_q_histogram /home/yuan/afl-target/aom/stats/rate_hist.c:255
    #2 0x55dcda8aade0 in main /home/yuan/afl-target/aom/apps/aomenc.c:2843
    #3 0x7f9667fc2bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #4 0x55dcda8bd739 in _start (/home/yuan/afl-target/aom/build/aomenc+0x93739)

Address 0x7ffce729bd78 is located in stack of thread T0 at offset 88 in frame
    #0 0x55dcda908b4f in show_q_histogram /home/yuan/afl-target/aom/stats/rate_hist.c:237

  This frame has 2 object(s):
    [32, 36) 'buckets'
    [96, 864) 'bucket' <== Memory access at offset 88 underflows this variable
HINT: this may be a false positive if your program uses some custom stack unwind mechanism or swapcontext
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/yuan/afl-target/aom/stats/rate_hist.c:185 in show_histogram
Shadow bytes around the buggy address:
  0x10001ce4b750: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001ce4b760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001ce4b770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001ce4b780: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001ce4b790: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10001ce4b7a0: 00 00 00 00 f1 f1 f1 f1 04 f2 f2 f2 f2 f2 f2[f2]
  0x10001ce4b7b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001ce4b7c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x10001ce4b7d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001ce4b7e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001ce4b7f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==7890==ABORTING
```

What version / commit were you testing with?
commit a5d214

poc2
2.1 KB View Download

Comment 1 by zodf0...@gmail.com on Tue, Dec 29, 2020, 2:17 AM EST

This is environment:
OS : ubuntu 18.04.3
kernel : gnu/linux 5.4.0-52-generic
CPU : Intel(R) Core(TM) i7-10700 CPU @ 2.90GHz
compiler : gcc version 7.5.0

This is How I build
1. git clone https://aomedia.googlesource.com/aom
2. cd aom/build
3. cmake ..

Comment 2 by jz...@google.com on Mon, Jan 11, 2021, 1:50 PM EST

Owner: huisu@google.com

Comment 3 by jz...@google.com on Mon, Jan 11, 2021, 1:50 PM EST

Status: Assigned (was: New)

Comment 4 by huisu@google.com on Mon, Jan 11, 2021, 4:17 PM EST

I noticed this:
Warning: Assuming --pass=2 implies --passes=2
Warning: Enforcing one-pass encoding in realtime mode

Did you want to use 2-pass mode or 1-pass mode?

Also, is the file poc2 a valid input?

Comment 5 by zodf0...@gmail.com on Mon, Jan 11, 2021, 8:58 PM EST

I check #2910 ~ #2914, the valid input can reproduce the problem.
I use the fuzzer to generate these problem, maybe the problem is because of the wrong usage at aomenc likely `--pass=2 --usage=1`.

Comment 6 Deleted

Comment 7 Deleted

Comment 8 by zodf0...@gmail.com on Tue, Jan 12, 2021, 1:48 AM EST

This is the valid mp4 file can trigger this problem.

small_movie.mp4
1.2 KB View Download

Comment 9 by bugdroid on Wed, Jan 13, 2021, 6:02 PM EST

The following revision refers to this bug:
https://aomedia.googlesource.com/aom/+/94bcbfe76b0fd5b8ac03645082dc23a88730c949

commit 94bcbfe76b0fd5b8ac03645082dc23a88730c949
Author: Hui Su <huisu@google.com>
Date: Wed Jan 13 23:01:41 2021

aomenc: initalize the image object

Otherwise it would cause problem when calling aom_img_free() at the end
if no frame is read.

~~BUG=aomedia:2911~~

Change-Id: I4350d5294706d2d84341e601e9ed6063229d0451

[modify] https://crrev.com/94bcbfe76b0fd5b8ac03645082dc23a88730c949/apps/aomenc.c

Comment 10 by jz...@google.com on Mon, Feb 8, 2021, 3:48 PM EST
Labels: Hotlist-AOM-OKR

Comment 11 by huisu@google.com on Fri, Apr 9, 2021, 5:21 PM EDT
Cc: huisu@google.com
~~Issue 2910~~ has been merged into this issue.

Comment 12 by huisu@google.com on Fri, Apr 9, 2021, 5:22 PM EDT
Status: Fixed (was: Assigned)