☆ Starred by 7 users

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

CC: ----

Status: Duplicate *(Closed)*

MergedInto: ~~Issue 2911~~

Components: ----

Modified: Apr 9, 2021

Type-Defect
Priority-Medium
Hotlist-AOM-OKR

Issue 2910: Null pointer dereference in rate_hist.c:264

Reported by zodf0...@gmail.com on Wed, Dec 23, 2020, 11:03 PM EST

Code ‹ Prev 391 of 2974 Next ›
Back to list

What version / commit were you testing with?
commit a5d214

What steps will reproduce the problem?

1. ./aomenc --pass=2 --rt --rate-hist=5 -o /dev/null ./poc1

What is the expected output?

This is ASAN report:

~~~
```

➜ Yuan-fuzz ~/aom/build/aomenc --pass=2 --rt --rate-hist=5 -o /dev/null ./poc1
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.

ASAN:DEADLYSIGNAL
================================================================
==6848==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000018 (pc 0x55ba5969e3a0 bp 0x000000000018 sp 0x7ffcc9f6f360 T0)
==6848==The signal is caused by a READ memory access.
==6848==Hint: address points to the zero page.
   #0 0x55ba5969e39f in show_rate_histogram /home/yuan/afl-target/aom/stats/rate_hist.c:264
   #1 0x55ba5963ff95 in main /home/yuan/afl-target/aom/apps/aomenc.c:2849
   #2 0x7fb5f3efabf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
   #3 0x55ba59652739 in _start (/home/yuan/afl-target/aom/build/aomenc+0x93739)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/yuan/afl-target/aom/stats/rate_hist.c:264 in show_rate_histogram
==6848==ABORTING

```
~~~

poc1
2.1 KB View Download

Comment 1 by jz...@google.com on Mon, Jan 11, 2021, 1:49 PM EST Project Member

Status: Assigned (was: New)
Owner: huisu@google.com

Comment 2 by jz...@google.com on Mon, Feb 8, 2021, 3:48 PM EST Project Member

Labels: Hotlist-AOM-OKR

Comment 3 by huisu@google.com on Fri, Apr 9, 2021, 5:21 PM EDT Project Member

Status: Duplicate (was: Assigned)
Mergedinto: 2911