☆ Starred by 3 users

Owner: yunqingwang@google.com

CC: jianj@google.com

Status: Fixed *(Closed)*

Components: ----

Modified: Mar 6, 2021

Type-Defect
Priority-Medium
Needs-Feedback

Issue 2914: SEGV on unknown address in aom_dsp/x86/obmc_sad_avx2.c:83

Reported by zodf0...@gmail.com on Thu, Dec 24, 2020, 1:43 AM EST

Code 1 of 99
Back to list

What version / commit were you testing with?
commit a5d214

What steps will reproduce the problem?
1. ./aomenc --rt --use-16bit-internal -h 10 -w 10 -o /dev/null ./poc5

What is the expected output?

This is the ASAN report:

~~~
```
➜  Yuan-fuzz ~/aom/build/aomenc --rt --use-16bit-internal -h 10 -w 10 -o /dev/null ./poc5
Warning: non-zero lag-in-frames option ignored in realtime mode.

Pass 1/1 frame    2/1        294B   28745 us 69.58 fps [ETA  0:00:00] ASAN:DEADLYSIGNAL
=================================================================
==20096==ERROR: AddressSanitizer: SEGV on unknown address 0x3f8bdc249d01 (pc 0x563cecce5ce7 bp 0x7ffd25466ad0 sp 0x7ffd25466ac0 T0)
==20096==The signal is caused by a READ memory access.
    #0 0x563cecce5ce6 in _mm256_lddqu_si256 /usr/lib/gcc/x86_64-linux-gnu/7/include/avxintrin.h:1004
    #1 0x563cecce5ce6 in obmc_sad_w8n_avx2 /home/yuan/afl-target/aom/aom_dsp/x86/obmc_sad_avx2.c:83
    #2 0x563cecce5ce6 in aom_obmc_sad16x8_avx2 /home/yuan/afl-target/aom/aom_dsp/x86/obmc_sad_avx2.c:133
    #3 0x563cebbcb4b5 in obmc_diamond_search_sad /home/yuan/afl-target/aom/av1/encoder/mcomp.c:2128
    #4 0x563cebc0a04c in obmc_full_pixel_diamond /home/yuan/afl-target/aom/av1/encoder/mcomp.c:2168
    #5 0x563cebc0a04c in av1_obmc_full_pixel_search /home/yuan/afl-target/aom/av1/encoder/mcomp.c:2216
    #6 0x563ced1717a0 in av1_single_motion_search /home/yuan/afl-target/aom/av1/encoder/motion_search_facade.c:232
    #7 0x563cebd80970 in motion_mode_rd /home/yuan/afl-target/aom/av1/encoder/rdopt.c:1369
    #8 0x563cebda373c in handle_inter_mode /home/yuan/afl-target/aom/av1/encoder/rdopt.c:2833
    #9 0x563cebdf6c13 in av1_rd_pick_inter_mode /home/yuan/afl-target/aom/av1/encoder/rdopt.c:5462
    #10 0x563ced1c14c1 in pick_sb_modes /home/yuan/afl-target/aom/av1/encoder/partition_search.c:685
    #11 0x563ced1e5e5f in rd_try_subblock /home/yuan/afl-target/aom/av1/encoder/partition_search.c:2220
    #12 0x563ced1e5e5f in rd_test_partition3 /home/yuan/afl-target/aom/av1/encoder/partition_search.c:2269
    #13 0x563ced1e5e5f in rd_pick_ab_part /home/yuan/afl-target/aom/av1/encoder/partition_search.c:2712
    #14 0x563ced1e5e5f in ab_partitions_search /home/yuan/afl-target/aom/av1/encoder/partition_search.c:2918
    #15 0x563ced1e5e5f in av1_rd_pick_partition /home/yuan/afl-target/aom/av1/encoder/partition_search.c:3690
    #16 0x563ced1dec18 in split_partition_search /home/yuan/afl-target/aom/av1/encoder/partition_search.c:3403
    #17 0x563ced1dec18 in av1_rd_pick_partition /home/yuan/afl-target/aom/av1/encoder/partition_search.c:3640
    #18 0x563ced1dec18 in split_partition_search /home/yuan/afl-target/aom/av1/encoder/partition_search.c:3403
    #19 0x563ced1dec18 in av1_rd_pick_partition /home/yuan/afl-target/aom/av1/encoder/partition_search.c:3640
    #20 0x563ced1dec18 in split_partition_search /home/yuan/afl-target/aom/av1/encoder/partition_search.c:3403
    #21 0x563ced1dec18 in av1_rd_pick_partition /home/yuan/afl-target/aom/av1/encoder/partition_search.c:3640
    #22 0x563ced071867 in encode_rd_sb /home/yuan/afl-target/aom/av1/encoder/encodeframe.c:710
    #23 0x563ced07bae9 in encode_sb_row /home/yuan/afl-target/aom/av1/encoder/encodeframe.c:848
    #24 0x563ced07bae9 in av1_encode_sb_row /home/yuan/afl-target/aom/av1/encoder/encodeframe.c:957
~~~

```
    #25 0x563ced07e5a4 in av1_encode_tile /home/yuan/afl-target/aom/av1/encoder/encodeframe.c:997
    #26 0x563ced086c3d in encode_tiles /home/yuan/afl-target/aom/av1/encoder/encodeframe.c:1027
    #27 0x563ced086c3d in encode_frame_internal /home/yuan/afl-target/aom/av1/encoder/encodeframe.c:1430
    #28 0x563ced08c9d9 in av1_encode_frame /home/yuan/afl-target/aom/av1/encoder/encodeframe.c:1598
    #29 0x563cebaa998b in encode_without_recode /home/yuan/afl-target/aom/av1/encoder/encoder.c:2317
    #30 0x563cebaa998b in encode_with_recode_loop_and_filter /home/yuan/afl-target/aom/av1/encoder/encoder.c:2610
    #31 0x563cebaba398 in encode_frame_to_data_rate /home/yuan/afl-target/aom/av1/encoder/encoder.c:3097
    #32 0x563cebaf650d in av1_encode /home/yuan/afl-target/aom/av1/encoder/encoder.c:3231
    #33 0x563ced125d3d in av1_encode_strategy /home/yuan/afl-target/aom/av1/encoder/encode_strategy.c:1356
    #34 0x563cebaf87d4 in av1_get_compressed_data /home/yuan/afl-target/aom/av1/encoder/encoder.c:3512
    #35 0x563ceb91eaec in encoder_encode /home/yuan/afl-target/aom/av1/av1_cx_iface.c:2313
    #36 0x563ceb7c462c in aom_codec_encode /home/yuan/afl-target/aom/aom/src/aom_encoder.c:155
    #37 0x563ceb5d90e1 in encode_frame /home/yuan/afl-target/aom/apps/aomenc.c:2064
    #38 0x563ceb5b7a7e in main /home/yuan/afl-target/aom/apps/aomenc.c:2711
    #39 0x7f17bb8b0bf6 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21bf6)
    #40 0x563ceb5cd739 in _start (/home/yuan/afl-target/aom/build/aomenc+0x93739)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /usr/lib/gcc/x86_64-linux-gnu/7/include/avxintrin.h:1004 in _mm256_lddqu_si256
==20096==ABORTING
```

By the way, could I try to report bugs I found to get CVE?

poc5
2.1 KB View Download

Comment 1 Deleted

Comment 2 by yaowu@google.com on Mon, Dec 28, 2020, 2:17 PM EST

thanks for reporting the issues.

Yes, please report issues found with CVE. Also it would be very much appreciated if you provide step-by-step instructions to reproduce, eg, git#, cmake options and run-time arguments etc.

Comment 3 by zodf0...@gmail.com on Tue, Dec 29, 2020, 2:05 AM EST

I'm sorry I forget to give CMake options .
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 ..

I also use valgrind to prove it

```
➜  build git:(master) ✗ valgrind ./aomenc --rt --use-16bit-internal -h 10 -w 10 -o /dev/null ~/Downloads/poc5
==6757== Memcheck, a memory error detector
==6757== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==6757== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==6757== Command: ./aomenc --rt --use-16bit-internal -h 10 -w 10 -o /dev/null /home/yuan/Downloads/poc5
==6757==
Warning: non-zero lag-in-frames option ignored in realtime mode.

Pass 1/1 frame    2/1        294B  634324 us 3.15 fps [ETA  0:00:08] ==6757== Invalid read of size 8
==6757==    at 0x8D5E11: aom_obmc_sad16x8_avx2 (in /home/yuan/aom/build/aomenc)
==6757==    by 0x269157: obmc_diamond_search_sad (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2709FC: av1_obmc_full_pixel_search (in /home/yuan/aom/build/aomenc)
==6757==    by 0x99BEFE: av1_single_motion_search (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2BB87B: motion_mode_rd (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2C2EE1: handle_inter_mode.constprop.39 (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2D1B9E: av1_rd_pick_inter_mode (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9A8E2A: pick_sb_modes (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9AEACE: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9ADA0C: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9ADA0C: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9ADA0C: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==  Address 0x340ac71 is not stack'd, malloc'd or (recently) free'd
==6757==
==6757==
==6757== Process terminating with default action of signal 11 (SIGSEGV)
==6757==  Access not within mapped region at address 0x340AC71
==6757==    at 0x8D5E11: aom_obmc_sad16x8_avx2 (in /home/yuan/aom/build/aomenc)
==6757==    by 0x269157: obmc_diamond_search_sad (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2709FC: av1_obmc_full_pixel_search (in /home/yuan/aom/build/aomenc)
==6757==    by 0x99BEFE: av1_single_motion_search (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2BB87B: motion_mode_rd (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2C2EE1: handle_inter_mode.constprop.39 (in /home/yuan/aom/build/aomenc)
==6757==    by 0x2D1B9E: av1_rd_pick_inter_mode (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9A8E2A: pick_sb_modes (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9AEACE: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9ADA0C: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9ADA0C: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==    by 0x9ADA0C: av1_rd_pick_partition (in /home/yuan/aom/build/aomenc)
==6757==  If you believe this happened as a result of a stack
==6757==  overflow in your program's main thread (unlikely but
==6757==  possible), you can try to increase the size of the
==6757==  main thread stack using the --main-stacksize= flag.
==6757==  The main thread stack size used in this run was 8388608.
==6757==
==6757== HEAP SUMMARY:
==6757==     in use at exit: 13,070,828 bytes in 357 blocks
==6757==   total heap usage: 1,329 allocs, 972 frees, 14,210,282 bytes allocated
==6757==
==6757== LEAK SUMMARY:
==6757==    definitely lost: 0 bytes in 0 blocks
==6757==    indirectly lost: 0 bytes in 0 blocks
```

```
==6757==      possibly lost: 12,965,500 bytes in 329 blocks
==6757==    still reachable: 105,328 bytes in 28 blocks
==6757==                       of which reachable via heuristic:
==6757==                         newarray           : 24 bytes in 1 blocks
==6757==         suppressed: 0 bytes in 0 blocks
==6757== Rerun with --leak-check=full to see details of leaked memory
==6757==
==6757== For counts of detected and suppressed errors, rerun with: -v
==6757== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
[1]    6757 segmentation fault  valgrind ./aomenc --rt --use-16bit-internal -h 10 -w 10 -o /dev/null
```

Comment 4 by jz...@google.com on Mon, Jan 11, 2021, 1:51 PM EST

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

Comment 5 by kmalladi@google.com on Mon, Jan 11, 2021, 3:53 PM EST

Cc: yanqingwang@google.com

FYI.

Comment 6 by jz...@google.com on Mon, Feb 22, 2021, 2:47 PM EST

Owner: yunqingwang@google.com
Cc: -yanqingwang@google.com

Comment 7 by yunqingwang@google.com on Fri, Mar 5, 2021, 12:43 PM EST

Followed above steps, but couldn't reproduce the invalid memory access.

```
$ valgrind ./aomenc --rt --use-16bit-internal -h 10 -w 10 -o /dev/null ~/Downloads/poc5
==830026== Memcheck, a memory error detector
==830026== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==830026== Using Valgrind-3.16.1 and LibVEX; rerun with -h for copyright info
==830026== Command: ./aomenc --rt --use-16bit-internal -h 10 -w 10 -o /dev/null ~/Downloads/poc5
==830026==
Pass 1/1 frame   14/14      1775B    1014b/f   30420b/s   76962 ms (0.18 fps)
webmenc> Segment::Finalize failed.
Fatal: WebM writer finalization failed.
==830026==
==830026== HEAP SUMMARY:
==830026==     in use at exit: 73,946 bytes in 9 blocks
==830026==   total heap usage: 8,545 allocs, 8,536 frees, 66,340,471 bytes allocated
==830026==
==830026== LEAK SUMMARY:
==830026==    definitely lost: 0 bytes in 0 blocks
==830026==    indirectly lost: 0 bytes in 0 blocks
==830026==      possibly lost: 1,518 bytes in 2 blocks
==830026==    still reachable: 72,428 bytes in 7 blocks
==830026==         suppressed: 0 bytes in 0 blocks
==830026== Rerun with --leak-check=full to see details of leaked memory
==830026==
==830026== For lists of detected and suppressed errors, rerun with: -s
==830026== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

On my machine: gcc version 10.2.1 20210110

Do you still see the issue with current top-of-tree code?

Comment 8 by jianj@google.com on Fri, Mar 5, 2021, 1:09 PM EST

This looks similar to https://bugs.chromium.org/p/aomedia/issues/detail?id=2940 which has been fixed.

Comment 9 by yunqingwang@google.com on Fri, Mar 5, 2021, 1:13 PM EST

Yes, I agree. Thanks Jerome for pointing it out.

Comment 10 by yunqingwang@google.com on Fri, Mar 5, 2021, 1:13 PM EST

Cc: jianj@google.com

Comment 11 by jianj@google.com on Fri, Mar 5, 2021, 1:17 PM EST

Labels: Needs-Feedback

Could you please try with the latest code and see if it still happens?

Comment 12 by zodf0...@gmail.com on Sat, Mar 6, 2021, 12:15 AM EST

Is fixed now, thanks.

Comment 13 by yunqingwang@google.com on Sat, Mar 6, 2021, 1:45 PM EST

Status: Fixed (was: Assigned)