Ruby master - Bug #18918
Can't compile ruby master with AFL ASAN
07/15/2022 03:22 PM - m.aldo (Muhammad Aldo Firmansyah)

Description
On ubuntu 20.04, I want to compile ruby on master branch with AFL's afl-clang-fast but I got ASAN error

$ ruby -v
$ ruby 3.0.2p107 (2021-07-07 revision 0db68f0233) [x86_64-linux]
$ git rev-parse --short HEAD
$ 7424ea184f

Here is error I got when using yjit in configure

... ... linking miniruby afl-clang-fast 2.56b by <lszekeres@google.com>
generating encdb.h

=================================================================
== 101657 ==
ERROR: AddressSanitizer: heap-use-after-free on address 0x6130000217d0
thread T0
WRITE of size 8 at 0x6130000217d0
SCARINESS: 52 (8-byte-write-heap-use-after-free)
#0 0x5555555de514 (/home/aldo/ruby/miniruby+0x88a514)
#1 0x5555555df3f411 (/home/aldo/ruby/miniruby+0x7eb411)
#2 0x55555555a231 (/home/aldo/ruby/miniruby+0x866231)
#3 0x5555556279ed3b (/home/aldo/ruby/miniruby+0xd25ed3b)
#4 0x55555555a32db (/home/aldo/ruby/miniruby+0x85f2db)
#5 0x55555555a7ef (/home/aldo/ruby/miniruby+0xa53fe5)
#6 0x5555555a4e6f4 (/home/aldo/ruby/miniruby+0x4f46f4)
#7 0x55555555a9e628 (/home/aldo/ruby/miniruby+0xa4a628)
#8 0x55555555b08ab (/home/aldo/ruby/miniruby+0xb45ab)
#9 0x55555555b6657 (/home/aldo/ruby/miniruby+0x6ab657)
#10 0x55555555bfbad5 (/home/aldo/ruby/miniruby+0x6a7ad5)
#11 0x55555555b37b88 (/home/aldo/ruby/miniruby+0x2837b88)
#12 0x55555555b1d80e (/home/aldo/ruby/miniruby+0xc80a80e)
#13 0x55555555b2cde (/home/aldo/ruby/miniruby+0xc8cde)
#14 0x55555555b2f38 (/home/aldo/ruby/miniruby+0xc8e3f38)
#15 0x55555555b1378 (/home/aldo/ruby/miniruby+0xc6d378)
#16 0x55555555b34e4 (/home/aldo/ruby/miniruby+0xc0e94e4)
#17 0x55555555b42e1 (/home/aldo/ruby/miniruby+0x4ee3e1)
#18 0x55555555b41bc5 (/home/aldo/ruby/miniruby+0x4edcb5)
#19 0x55555555b78fa5 (/home/aldo/ruby/miniruby+0x285fa5)
#20 0x7ffffff7b8082 (/lib/x86_64-linux-gnu/libc.so.6+0x24082)
#21 0x55555555b31f7d (/home/aldo/ruby/miniruby+0x1ddfd7)

0x6130000217d0 is located 16 bytes inside of 336-byte region [0x6130000217c0,0x61300002190]
freed by thread T0 here:
#0 0x55555557a43d (/home/aldo/ruby/miniruby+0x25643d)
#1 0x55555557abc166 (/home/aldo/ruby/miniruby+0x568166)

previously allocated by thread T0 here:
#0 0x55555557a832 (/home/aldo/ruby/miniruby+0x256832)
SUMMARY: AddressSanitizer: heap-use-after-free (/home/aldo/ruby/miniruby+0x88a514)

Shadow bytes around the buggy address:
0x0c267fffc2a0: 00 00 00 00 00 00 00 00
0x0c267fffc2b0: 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c267fffc2c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c267fffc2d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c267fffc2e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c267fffc2f0: fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd fd
0x0c267fffc300: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c267fffc310: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c267fffc320: fd fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c267fffc330: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c267fffc340: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd

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
--101657==ABORTING
make: *** Waiting for unfinished jobs....
/bin/sh ./tool/ifchange "--timestamp=.rbconfig.time" rbconfig.rb rbconfig.tmp
rbconfig.rb updated

And Here is error I got when not using yjit in configure

... ...
./revision.h unchanged
linking miniruby
afl-clang-fast 2.56b by <lszekeres@google.com>
genarating encdb.h

---124261==
ERROR: AddressSanitizer: use-after-poison on address 0x7ffffff4a0068 at pc 0x5555555f7ab5 bp 0x7ffffffb5e0 sp 0x7ffffffb5d8
READ of size 8 at 0x7ffffff4a0068 thread T0
SCARINESS: 33 (8-byte-read-use-after-poison)
#0 0x5555555f7ab4   (/home/aldo/ruby/miniruby+0xaaa3ab4)
Address 0x7fff40a00068 is a wild pointer.

SUMMARY: AddressSanitizer: use-after-poison (/home/aldo/ruby/miniruby+0xa3ab4)

Shadow bytes around the buggy address:

0x10007e80bfb0: 00 00 00 f7 00 00 00 00 f7 00 00 00 f7 00 00 00
0x10007e80bfc0: 00 00 f7 00 00 00 00 f7 00 00 00 00 f7 00 00 00
0x10007e80bfd0: 00 f7 00 00 00 00 f7 00 00 00 00 f7 00 00 00
0x10007e80bfe0: f7 00 00 00 00 f7 00 00 00 00 f7 00 00 00 00
0x10007e80bff0: 00 00 00 00 f7 00 00 00 00 f7 00 00 00
0x10007e80c000: 00 00 00 f7 00 00 00 00 f7 00 00 00 00 f7 00 00 00
0x10007e80c010: 00 00 f7 00 00 00 00 f7 00 00 00 00 f7 00 00 00
0x10007e80c020: 00 f7 00 00 00 00 f7 00 00 00 00 f7 00 00 00
0x10007e80c030: f7 00 00 00 00 f7 00 00 00 00 f7 00 00 00 00
0x10007e80c040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f7 00
0x10007e80c050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f7 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
Shadow gap: cc
make: *** Waiting for unfinished jobs....
/bin/sh ./tool/ifchange "--timestamp=.rbconfig.time" rbconfig.rb rbconfig.tmp
rbconfig.rb updated