

Ruby - Bug #21332

heap-use-after-free caused by mutating the set

05/13/2025 12:19 PM - cyruscyliu (Qiang Liu)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 3.5.0dev (2025-05-13T08:35:34Z master a6435befa7) +PRISM [x86_64-linux]	Backport: 3.2: UNKNOWN, 3.3: UNKNOWN, 3.4: UNKNOWN

Description

Hi, we found a heap-use-after-free caused by mutating the set.

hash() returning 0 is important to create the collision and then trigger eql?

```
$flag = false
$c = 0
class C
  def hash
    return 0
  end

  def eql?(other)
    if $flag
      if $c == 0
        $c += 1
        $a.merge((1...10).map {C.new})
        return false
      end
    end
    end
end

$a = Set.new((1..10).map { |o| C.new })
$a.delete_if { |x|
  if $c == 0
    $a.delete($a.to_a[0])
  end
  $flag = true
}
```

```
$ git log | head -n4
commit a6435befa76c2ae0525147f934bd9cd1914fffb8a
Author: Jean Boussier <jean.boussier@gmail.com>
Date: Mon May 12 11:02:17 2025 +0200
$ ./ruby triaged/set_delete_if.rb
`RubyGems' were not loaded.
`error_highlight' was not loaded.
`did_you_mean' was not loaded.
`syntax_suggest' was not loaded.
=====
==229421==ERROR: AddressSanitizer: heap-use-after-free on address 0x511000009dd0 at pc 0x632e6e7fc
01d bp 0x7fffb8fd7170 sp 0x7fffb8fd7168
READ of size 8 at 0x511000009dd0 thread T0
#0 0x632e6e7fc01c in set_general_foreach /media/test/ruby/build/./st.c:3047:13
#1 0x632e6e8026ff in set_foreach_call /media/test/ruby/build/./set.c:329:11
#2 0x632e6e59e5c6 in rb_ensure /media/test/ruby/build/./eval.c:1074:18
#3 0x632e6e80247c in set_iter /media/test/ruby/build/./set.c:352:9
#4 0x632e6e7ff9f4 in set_i_delete_if /media/test/ruby/build/./set.c:769:5
#5 0x632e6e93a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_inshelper.c:3798:
11
```

```

#6 0x632e6e92304a in vm_call_method_each_type /media/test/ruby/build/./vm_insnhelper.c:4776:1
6
#7 0x632e6e922b13 in vm_call_method /media/test/ruby/build/./vm_insnhelper.c
#8 0x632e6e8ea539 in vm_sendish /media/test/ruby/build/./vm_insnhelper.c:5995:15
#9 0x632e6e8ea539 in vm_exec_core /media/test/ruby/build/./insns.def:851:11
#10 0x632e6e8dfcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#11 0x632e6e59bbf0 in rb_ec_exec_node /media/test/ruby/build/./eval.c:281:9
#12 0x632e6e59bbf0 in ruby_run_node /media/test/ruby/build/./eval.c:319:30
#13 0x632e6e5972b0 in rb_main /media/test/ruby/build/./main.c:42:12
#14 0x632e6e5972b0 in main /media/test/ruby/build/./main.c:62:12
#15 0x7a1fdf62a1c9 in __libc_start_call_main csu/./sysdeps/nptl/libc_start_call_main.h:58:16
#16 0x7a1fdf62a28a in __libc_start_main csu/./csu/libc-start.c:360:3
#17 0x632e6e4bdd94 in _start (/media/test/ruby/build/ruby+0x14bd94) (BuildId: 5c3c6444d00499cf
0254892dbef6454db4a9698a)

0x511000009dd0 is located 16 bytes inside of 256-byte region [0x511000009dc0,0x511000009ec0)
freed by thread T0 here:
#0 0x632e6e55894a in free (/media/test/ruby/build/ruby+0x1e694a) (BuildId: 5c3c6444d00499cf025
4892dbef6454db4a9698a)
#1 0x632e6e5c344b in rb_gc_impl_free /media/test/ruby/build/./gc/default/default.c:8099:9
#2 0x632e6e5c344b in ruby_sized_xfree /media/test/ruby/build/./gc.c:5225:13
#3 0x632e6e5c344b in ruby_xfree /media/test/ruby/build/./gc.c:5236:5
#4 0x632e6e7f94eb in set_rebuild_move_table /media/test/ruby/build/./st.c:2592:5
#5 0x632e6e7f94eb in set_rebuild_table /media/test/ruby/build/./st.c:2542:9
#6 0x632e6e7f94eb in set_rebuild_table_if_necessary /media/test/ruby/build/./st.c:2876:9
#7 0x632e6e7f94eb in rb_set_insert /media/test/ruby/build/./st.c:2894:5
#8 0x632e6e802b4b in set_table_insert_wb /media/test/ruby/build/./set.c:378:15
#9 0x632e6e802b4b in set_merge_enum_into /media/test/ruby/build/./set.c:1121:13
#10 0x632e6e800a1f in set_i_merge /media/test/ruby/build/./set.c:1147:9
#11 0x632e6e93a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_insnhelper.c:3798
:11
#12 0x632e6e92304a in vm_call_method_each_type /media/test/ruby/build/./vm_insnhelper.c:4776:
16
#13 0x632e6e922b13 in vm_call_method /media/test/ruby/build/./vm_insnhelper.c
#14 0x632e6e8e76f3 in vm_sendish /media/test/ruby/build/./vm_insnhelper.c:5995:15
#15 0x632e6e8e76f3 in vm_exec_core /media/test/ruby/build/./insns.def:899:11
#16 0x632e6e8dfcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#17 0x632e6e94dcad in vm_call0_body /media/test/ruby/build/./vm_eval.c:225:20
#18 0x632e6e905fa6 in vm_call0_cc /media/test/ruby/build/./vm_eval.c:101:12
#19 0x632e6e905fa6 in rb_funcallv_scope /media/test/ruby/build/./vm_eval.c:1064:16
#20 0x632e6e906c53 in rb_funcallv /media/test/ruby/build/./vm_eval.c:1079:12
#21 0x632e6e906c53 in rb_funcall /media/test/ruby/build/./vm_eval.c:1136:12
#22 0x632e6e6d443b in rb_eq1 /media/test/ruby/build/./object.c:199:18
#23 0x632e6e608cfb in rb_any_cmp /media/test/ruby/build/./hash.c:142:13
#24 0x632e6e7fb7c4 in set_find_entry /media/test/ruby/build/./st.c:2639:9
#25 0x632e6e7fb7c4 in set_general_foreach /media/test/ruby/build/./st.c:3098:23
#26 0x632e6e8026ff in set_foreach_call /media/test/ruby/build/./set.c:329:11
#27 0x632e6e59e5c6 in rb_ensure /media/test/ruby/build/./eval.c:1074:18
#28 0x632e6e80247c in set_iter /media/test/ruby/build/./set.c:352:9
#29 0x632e6e7ff9f4 in set_i_delete_if /media/test/ruby/build/./set.c:769:5
#30 0x632e6e93a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_insnhelper.c:3798
:11
#31 0x632e6e92304a in vm_call_method_each_type /media/test/ruby/build/./vm_insnhelper.c:4776:
16
#32 0x632e6e922b13 in vm_call_method /media/test/ruby/build/./vm_insnhelper.c
#33 0x632e6e8ea539 in vm_sendish /media/test/ruby/build/./vm_insnhelper.c:5995:15
#34 0x632e6e8ea539 in vm_exec_core /media/test/ruby/build/./insns.def:851:11
#35 0x632e6e8dfcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#36 0x632e6e59bbf0 in rb_ec_exec_node /media/test/ruby/build/./eval.c:281:9
#37 0x632e6e59bbf0 in ruby_run_node /media/test/ruby/build/./eval.c:319:30
#38 0x632e6e5972b0 in rb_main /media/test/ruby/build/./main.c:42:12
#39 0x632e6e5972b0 in main /media/test/ruby/build/./main.c:62:12
#40 0x7a1fdf62a1c9 in __libc_start_call_main csu/./sysdeps/nptl/libc_start_call_main.h:58:16
#41 0x7a1fdf62a28a in __libc_start_main csu/./csu/libc-start.c:360:3
#42 0x632e6e4bdd94 in _start (/media/test/ruby/build/ruby+0x14bd94) (BuildId: 5c3c6444d00499cf
0254892dbef6454db4a9698a)

```

```

previously allocated by thread T0 here:
#0 0x632e6e558be3 in malloc (/media/test/ruby/build/ruby+0x1e6be3) (BuildId: 5c3c6444d00499cf0
254892dbef6454db4a9698a)
#1 0x632e6e5ffdf5 in rb_gc_impl_malloc /media/test/ruby/build/./gc/default/default.c:8114:5
#2 0x632e6e5ce9f2 in ruby_xmalloc_body /media/test/ruby/build/./gc.c:5116:12
#3 0x632e6e5ce9f2 in ruby_xmalloc /media/test/ruby/build/./gc.c:5106:34
#4 0x632e6e7f8586 in set_init_existing_table_with_size /media/test/ruby/build/./st.c:2442:40
#5 0x632e6e7f8586 in rb_set_init_table_with_size /media/test/ruby/build/./st.c:2457:5
#6 0x632e6e7f93d5 in set_rebuild_table /media/test/ruby/build/./st.c:2539:19
#7 0x632e6e7f93d5 in set_rebuild_table_if_necessary /media/test/ruby/build/./st.c:2876:9
#8 0x632e6e7f93d5 in rb_set_insert /media/test/ruby/build/./st.c:2894:5
#9 0x632e6e7fdfdb in set_table_insert_wb /media/test/ruby/build/./set.c:378:15
#10 0x632e6e7fdfdb in set_i_initialize /media/test/ruby/build/./set.c:503:17
#11 0x632e6e93a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_insnhelper.c:3798
:11
#12 0x632e6e92304a in vm_call_method_each_type /media/test/ruby/build/./vm_insnhelper.c:4776:
16
#13 0x632e6e922b13 in vm_call_method /media/test/ruby/build/./vm_insnhelper.c
#14 0x632e6e8e76f3 in vm_sendish /media/test/ruby/build/./vm_insnhelper.c:5995:15
#15 0x632e6e8e76f3 in vm_exec_core /media/test/ruby/build/./insns.def:899:11
#16 0x632e6e8dfcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#17 0x632e6e59bbf0 in rb_ec_exec_node /media/test/ruby/build/./eval.c:281:9
#18 0x632e6e59bbf0 in ruby_run_node /media/test/ruby/build/./eval.c:319:30
#19 0x632e6e5972b0 in rb_main /media/test/ruby/build/./main.c:42:12
#20 0x632e6e5972b0 in main /media/test/ruby/build/./main.c:62:12
#21 0x7a1fdf62a1c9 in __libc_start_call_main csu/./sysdeps/nptl/libc_start_call_main.h:58:16
#22 0x7a1fdf62a28a in __libc_start_main csu/./csu/libc-start.c:360:3
#23 0x632e6e4bdd94 in _start (/media/test/ruby/build/ruby+0x14bd94) (BuildId: 5c3c6444d00499cf
0254892dbef6454db4a9698a)

```

SUMMARY: AddressSanitizer: heap-use-after-free /media/test/ruby/build/./st.c:3047:13 in set_gener
al_foreach

Shadow bytes around the buggy address:

```

0x511000009b00: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x511000009b80: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x511000009c00: fd fd fd fa fa fa fa fa fa fa fa fa fa fa fa fa
0x511000009c80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x511000009d00: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa fa
=>0x511000009d80: fa fa fa fa fa fa fa fa fd fd[fd]fd fd fd fd fd fd
0x511000009e00: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x511000009e80: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa
0x511000009f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x511000009f80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x51100000a000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa

```

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

```

==229421==ABORTING

triaged/set_delete_if.rb:21: [BUG] ASAN error

ruby 3.5.0dev (2025-05-13T08:35:34Z master a6435befa7) +PRISM [x86_64-linux]

```

-- Control frame information -----
c:0003 p:---- s:0010 e:000009 CFUNC  :delete_if
c:0002 p:0042 s:0006 e:000005 EVAL    triaged/set_delete_if.rb:21 [FINISH]
c:0001 p:0000 s:0003 E:000be0 DUMMY   [FINISH]

-- Ruby level backtrace information -----
triaged/set_delete_if.rb:21:in '<main>'
triaged/set_delete_if.rb:21:in 'delete_if'

-- Threading information -----
Total ractor count: 1
Ruby thread count for this ractor: 1

-- C level backtrace information -----
./ruby(__interceptor_backtrace) [0x632e6e5026aa]
/media/test/ruby/build/ruby(rb_print_backtrace+0x14) [0x632e6ec75c97] /media/test/ruby/build/./vm_dump.c:843
/media/test/ruby/build/ruby(rb_vm_bugreport) /media/test/ruby/build/./vm_dump.c:1175
/media/test/ruby/build/ruby(rb_bug_without_die_internal+0x23c) [0x632e6ebca16c] /media/test/ruby/build/./error.c:1097
/media/test/ruby/build/ruby(rb_bug_without_die+0x127) [0x632e6ebc9e87] /media/test/ruby/build/./error.c:1106
./ruby(0x632e6e57d2aa) [0x632e6e57d2aa]
./ruby(0x632e6e55da2f) [0x632e6e55da2f]
./ruby(0x632e6e560ab5) [0x632e6e560ab5]
./ruby(__asan_report_load8) [0x632e6e56181c]
/media/test/ruby/build/ruby(set_general_foreach+0x120d) [0x632e6e7fc01d] /media/test/ruby/build/./st.c:3047
/media/test/ruby/build/ruby(set_foreach_call+0x40) [0x632e6e802700] /media/test/ruby/build/./set.c:329
/media/test/ruby/build/ruby(rb_ensure+0x257) [0x632e6e59e5c7] /media/test/ruby/build/./eval.c:1074
/media/test/ruby/build/ruby(set_iter+0x28d) [0x632e6e80247d] /media/test/ruby/build/./set.c:352
/media/test/ruby/build/ruby(iter_lev_in_flags+0x0) [0x632e6e7ff9f5] /media/test/ruby/build/./set.c:769
/media/test/ruby/build/ruby(set_iterating_p) /media/test/ruby/build/./set.c:243
/media/test/ruby/build/ruby(set_compact_after_delete) /media/test/ruby/build/./set.c:366
/media/test/ruby/build/ruby(set_i_delete_if) /media/test/ruby/build/./set.c:770
/media/test/ruby/build/ruby(vm_cfp_consistent_p+0x0) [0x632e6e93a9dc] ../vm_insnhelper.c:3798
/media/test/ruby/build/ruby(vm_call_cfunc_with_frame_) ../vm_insnhelper.c:3800
/media/test/ruby/build/ruby(vm_call_method_each_type+0x27b) [0x632e6e92304b] ../vm_insnhelper.c:4776
./ruby(vm_call_method+0x2d4) [0x632e6e922b14]
/media/test/ruby/build/ruby(vm_sendish+0x11f) [0x632e6e8ea53a] ../vm_insnhelper.c:5995
/media/test/ruby/build/ruby(vm_exec_core) ../insns.def:851
./ruby(vm_exec_loop+0x0) [0x632e6e8dfcd8]
/media/test/ruby/build/ruby(rb_vm_exec) /media/test/ruby/build/./vm.c:2626
/media/test/ruby/build/ruby(rb_ec_exec_node+0x53) [0x632e6e59bbf1] /media/test/ruby/build/./eval.c:281
/media/test/ruby/build/ruby(ruby_run_node) /media/test/ruby/build/./eval.c:319
/media/test/ruby/build/ruby(rb_main+0x29) [0x632e6e5972b1] /media/test/ruby/build/./main.c:42
/media/test/ruby/build/ruby(main) /media/test/ruby/build/./main.c:62
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_call_main+0x7a) [0x7a1fdf62a1ca] ../sysdeps/nptl/libc_start_call_main.h:58
/lib/x86_64-linux-gnu/libc.so.6(call_init+0x0) [0x7a1fdf62a28b] ../csu/libc-start.c:360
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main_impl) ../csu/libc-start.c:347
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main) (null):0
./ruby(_start) [0x632e6e4bdd95]

-- Other runtime information -----

* Loaded script: triaged/set_delete_if.rb

* Loaded features:

  0 enumerator.so
  1 thread.rb

```

```
2 fiber.so
3 rational.so
4 complex.so
5 ruby2_keywords.rb
6 set.rb
```

Associated revisions

Revision 1ee4b43a - 05/13/2025 08:27 PM - byroot (Jean Boussier)

Set#merge: raise if called during iteration

[Bug #21332]

History

#1 - 05/13/2025 07:41 PM - byroot (Jean Boussier)

Set#merge is missing a check for iteration: <https://github.com/ruby/ruby/pull/13322>

#2 - 05/13/2025 08:27 PM - byroot (Jean Boussier)

- Status changed from Open to Closed

Applied in changeset [git|1ee4b43a56e9539d3b09c08114c59cb49857b956](https://github.com/ruby/ruby/pull/13322).

Set#merge: raise if called during iteration

[Bug [#21332](#)]