

Ruby - Bug #21331

heap-use-after-free caused by rehash during transform_values!

05/13/2025 12:18 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: REQUIRED, 3.3: DONE, 3.4: DONE

Description

Hi, we found a heap-use-after-free caused by rehash during transform_values!.

```
$a = (1..1337).to_h { |k| [k, k] }
$a.transform_values! { |v|
  $a.rehash
  v * 2
}
```

```
$ git log | head -n4
commit a6435befa76c2ae0525147f934bd9cd1914ffb8a
Author: Jean Boussier <jean.boussier@gmail.com>
Date: Mon May 12 11:02:17 2025 +0200
$ ./ruby triaged/hash_transform_values.rb
`RubyGems' were not loaded.
`error_highlight' was not loaded.
`did_you_mean' was not loaded.
`syntax_suggest' was not loaded.
=====
==225007==ERROR: AddressSanitizer: heap-use-after-free on address 0x52f00000e408 at pc 0x64e677315414 bp 0x7fff926378f0 sp 0x7fff926378e8
WRITE of size 8 at 0x52f00000e408 thread T0
#0 0x64e677315413 in st_general_foreach /media/test/ruby/build/./st.c:1560:33
#1 0x64e677133dce in rb_hash_stlike_foreach_with_replace /media/test/ruby/build/./hash.c:1425:16
#2 0x64e677133dce in rb_hash_transform_values_bang /media/test/ruby/build/./hash.c:3552:9
#3 0x64e67745a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_insnhelper.c:3798:11
#4 0x64e67744304a in vm_call_method_each_type /media/test/ruby/build/./vm_insnhelper.c:4776:16
#5 0x64e677442b13 in vm_call_method /media/test/ruby/build/./vm_insnhelper.c
#6 0x64e67740a539 in vm_sendish /media/test/ruby/build/./vm_insnhelper.c:5995:15
#7 0x64e67740a539 in vm_exec_core /media/test/ruby/build/./insns.def:851:11
#8 0x64e6773ffcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#9 0x64e6770bbbff0 in rb_ec_exec_node /media/test/ruby/build/./eval.c:281:9
#10 0x64e6770bbbff0 in ruby_run_node /media/test/ruby/build/./eval.c:319:30
#11 0x64e6770b72b0 in rb_main /media/test/ruby/build/./main.c:42:12
#12 0x64e6770b72b0 in main /media/test/ruby/build/./main.c:62:12
#13 0x7c2903e2a1c9 in __libc_start_call_main csu/./sysdeps/nptl/libc_start_call_main.h:58:16
#14 0x7c2903e2a28a in __libc_start_main csu/./csu/libc-start.c:360:3
#15 0x64e676fddd94 in _start (/media/test/ruby/build/ruby+0x14bd94) (BuildId: 5c3c6444d00499cf0254892dbef6454db4a9698a)
```

0x52f00000e408 is located 8 bytes inside of 49152-byte region [0x52f00000e400,0x52f00001a400) freed by thread T0 here:

```
#0 0x64e67707894a in free (/media/test/ruby/build/ruby+0x1e694a) (BuildId: 5c3c6444d00499cf0254892dbef6454db4a9698a)
#1 0x64e6770e344b in rb_gc_impl_free /media/test/ruby/build/./gc/default/default.c:8099:9
#2 0x64e6770e344b in ruby_sized_xfree /media/test/ruby/build/./gc.c:5225:13
#3 0x64e6770e344b in ruby_xfree /media/test/ruby/build/./gc.c:5236:5
#4 0x64e67712be09 in hash_st_free /media/test/ruby/build/./hash.c:1218:5
```

```

#5 0x64e67712be09 in rb_hash_rehash /media/test/ruby/build/./hash.c:2026:9
#6 0x64e67745a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_insnhelper.c:3798:
11
#7 0x64e67744304a in vm_call_method_each_type /media/test/ruby/build/./vm_insnhelper.c:4776:1
6
#8 0x64e677442b13 in vm_call_method /media/test/ruby/build/./vm_insnhelper.c
#9 0x64e6774076f3 in vm_sendish /media/test/ruby/build/./vm_insnhelper.c:5995:15
#10 0x64e6774076f3 in vm_exec_core /media/test/ruby/build/./insns.def:899:11
#11 0x64e6773ffcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#12 0x64e677475dcc in invoke_iseq_block_from_c /media/test/ruby/build/./vm.c:1653:12
#13 0x64e677475dcc in invoke_block_from_c_bh /media/test/ruby/build/./vm.c:1667:20
#14 0x64e677427cca in vm_yield_with_cref /media/test/ruby/build/./vm.c:1704:12
#15 0x64e677427cca in vm_yield /media/test/ruby/build/./vm.c:1712:12
#16 0x64e677427cca in rb_yield_0 /media/test/ruby/build/./vm_eval.c:1361:12
#17 0x64e677427cca in rb_yield /media/test/ruby/build/./vm_eval.c
#18 0x64e67713db0d in transform_values_foreach_replace /media/test/ruby/build/./hash.c:3482:2
3
#19 0x64e67731443d in st_general_foreach /media/test/ruby/build/./st.c:1559:22
#20 0x64e677133dce in rb_hash_stlike_foreach_with_replace /media/test/ruby/build/./hash.c:142
5:16
#21 0x64e677133dce in rb_hash_transform_values_bang /media/test/ruby/build/./hash.c:3552:9
#22 0x64e67745a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_insnhelper.c:3798
:11
#23 0x64e67744304a in vm_call_method_each_type /media/test/ruby/build/./vm_insnhelper.c:4776:
16
#24 0x64e677442b13 in vm_call_method /media/test/ruby/build/./vm_insnhelper.c
#25 0x64e67740a539 in vm_sendish /media/test/ruby/build/./vm_insnhelper.c:5995:15
#26 0x64e67740a539 in vm_exec_core /media/test/ruby/build/./insns.def:851:11
#27 0x64e6773ffcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#28 0x64e6770bbb0 in rb_ec_exec_node /media/test/ruby/build/./eval.c:281:9
#29 0x64e6770bbb0 in ruby_run_node /media/test/ruby/build/./eval.c:319:30
#30 0x64e6770b72b0 in rb_main /media/test/ruby/build/./main.c:42:12
#31 0x64e6770b72b0 in main /media/test/ruby/build/./main.c:62:12
#32 0x7c2903e2a1c9 in __libc_start_call_main csu/./sysdeps/nptl/libc_start_call_main.h:58:16
#33 0x7c2903e2a28a in __libc_start_main csu/./csu/libc-start.c:360:3
#34 0x64e676fddd94 in _start (/media/test/ruby/build/ruby+0x14bd94) (BuildId: 5c3c6444d00499cf
0254892dbef6454db4a9698a)

previously allocated by thread T0 here:
#0 0x64e677078be3 in malloc (/media/test/ruby/build/ruby+0x1e6be3) (BuildId: 5c3c6444d00499cf0
254892dbef6454db4a9698a)
#1 0x64e67711fdf5 in rb_gc_impl_malloc /media/test/ruby/build/./gc/default/default.c:8114:5
#2 0x64e6770ee9f2 in ruby_xmalloc_body /media/test/ruby/build/./gc.c:5116:12
#3 0x64e6770ee9f2 in ruby_xmalloc /media/test/ruby/build/./gc.c:5106:34
#4 0x64e67730e4a1 in rb_st_init_existing_table_with_size /media/test/ruby/build/./st.c:559:39
#5 0x64e6773105b0 in rb_st_init_table_with_size /media/test/ruby/build/./st.c:585:5
#6 0x64e6773105b0 in rebuild_table /media/test/ruby/build/./st.c:753:19
#7 0x64e6773105b0 in rebuild_table_if_necessary /media/test/ruby/build/./st.c:1125:9
#8 0x64e677310f6b in st_add_direct_with_hash /media/test/ruby/build/./st.c:1187:5
#9 0x64e677313cf3 in rb_st_update /media/test/ruby/build/./st.c:1502:13
#10 0x64e67712e018 in rb_hash_stlike_update /media/test/ruby/build/./hash.c:1686:12
#11 0x64e67712e018 in tbl_update /media/test/ruby/build/./hash.c:1727:15
#12 0x64e67712de82 in rb_hash_aset /media/test/ruby/build/./hash.c
#13 0x64e67712e510 in rb_hash_set_pair /media/test/ruby/build/./hash.c:3715:5
#14 0x64e6773fbbf3 in vm_yield_with_cfunc /media/test/ruby/build/./vm_insnhelper.c:5161:11
#15 0x64e6774757f9 in invoke_block_from_c_bh /media/test/ruby/build/./vm.c:1672:16
#16 0x64e677427cca in vm_yield_with_cref /media/test/ruby/build/./vm.c:1704:12
#17 0x64e677427cca in vm_yield /media/test/ruby/build/./vm.c:1712:12
#18 0x64e677427cca in rb_yield_0 /media/test/ruby/build/./vm_eval.c:1361:12
#19 0x64e677427cca in rb_yield /media/test/ruby/build/./vm_eval.c
#20 0x64e6772511c7 in range_each_fixnum_loop /media/test/ruby/build/./range.c:1059:9
#21 0x64e6772511c7 in range_each /media/test/ruby/build/./range.c:1096:16
#22 0x64e67746dfd5 in vm_call0_cfunc_with_frame /media/test/ruby/build/./vm_eval.c:164:15
#23 0x64e67746dfd5 in vm_call0_cfunc /media/test/ruby/build/./vm_eval.c:178:12
#24 0x64e67746dfd5 in vm_call0_body /media/test/ruby/build/./vm_eval.c:229:15
#25 0x64e677471a0a in vm_call0_cc /media/test/ruby/build/./vm_eval.c:101:12
#26 0x64e677471a0a in rb_call0 /media/test/ruby/build/./vm_eval.c:571:12

```

```

#27 0x64e6774295f5 in rb_call /media/test/ruby/build/./vm_eval.c:890:12
#28 0x64e6774295f5 in iterate_method /media/test/ruby/build/./vm_eval.c:1545:12
#29 0x64e677429bf5 in rb_iterate0 /media/test/ruby/build/./vm_eval.c:1487:18
#30 0x64e677429287 in rb_iterate_internal /media/test/ruby/build/./vm_eval.c:1519:12
#31 0x64e677429287 in rb_block_call_kw /media/test/ruby/build/./vm_eval.c:1568:12
#32 0x64e677429287 in rb_block_call /media/test/ruby/build/./vm_eval.c:1554:12
#33 0x64e6776c75e0 in enum_hashify_into /media/test/ruby/build/./enum.c:743:5
#34 0x64e6776c75e0 in enum_hashify /media/test/ruby/build/./enum.c:750:12
#35 0x64e6776c75e0 in enum_to_h /media/test/ruby/build/./enum.c:791:12
#36 0x64e67745a9db in vm_call_cfunc_with_frame_ /media/test/ruby/build/./vm_inshelper.c:3798
:11
#37 0x64e67744304a in vm_call_method_each_type /media/test/ruby/build/./vm_inshelper.c:4776:
16
#38 0x64e677442b13 in vm_call_method /media/test/ruby/build/./vm_inshelper.c
#39 0x64e67740a539 in vm_sendish /media/test/ruby/build/./vm_inshelper.c:5995:15
#40 0x64e67740a539 in vm_exec_core /media/test/ruby/build/./insns.def:851:11
#41 0x64e6773ffcd7 in rb_vm_exec /media/test/ruby/build/./vm.c
#42 0x64e6770bbb0 in rb_ec_exec_node /media/test/ruby/build/./eval.c:281:9
#43 0x64e6770bbb0 in ruby_run_node /media/test/ruby/build/./eval.c:319:30
#44 0x64e6770b72b0 in rb_main /media/test/ruby/build/./main.c:42:12
#45 0x64e6770b72b0 in main /media/test/ruby/build/./main.c:62:12
#46 0x7c2903e2alc9 in __libc_start_call_main csu/./sysdeps/nptl/libc_start_call_main.h:58:16
#47 0x7c2903e2a28a in __libc_start_main csu/./csu/libc-start.c:360:3
#48 0x64e676fddd94 in _start (/media/test/ruby/build/ruby+0x14bd94) (BuildId: 5c3c6444d00499cf
0254892dbef6454db4a9698a)

```

SUMMARY: AddressSanitizer: heap-use-after-free /media/test/ruby/build/./st.c:1560:33 in st_genera
l_foreach

Shadow bytes around the buggy address:

```

0x52f00000e180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x52f00000e200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x52f00000e280: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x52f00000e300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x52f00000e380: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x52f00000e400: fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x52f00000e480: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x52f00000e500: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x52f00000e580: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x52f00000e600: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x52f00000e680: 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:         fl
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

```

==225007==ABORTING

triaged/hash_transform_values.rb:3: [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 :transform_values!
c:0002 p:0016 s:0006 e:000005 EVAL triaged/hash_transform_values.rb:3 [FINISH]
c:0001 p:0000 s:0003 E:000be0 DUMMY [FINISH]

```

```

-- Ruby level backtrace information -----
triaged/hash_transform_values.rb:3:in '<main>'
triaged/hash_transform_values.rb:3:in 'transform_values!'

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

-- C level backtrace information -----
./ruby(__interceptor_backtrace) [0x64e6770226aa]
/media/test/ruby/build/ruby(rb_print_backtrace+0x14) [0x64e677795c97] /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) [0x64e6776ea16c] /media/test/ruby/build/./error.c:1097
/media/test/ruby/build/ruby(rb_bug_without_die+0x127) [0x64e6776e9e87] /media/test/ruby/build/./error.c:1106
./ruby(0x64e67709d2aa) [0x64e67709d2aa]
./ruby(0x64e67707da2f) [0x64e67707da2f]
./ruby(0x64e677080ab5) [0x64e677080ab5]
./ruby(__asan_report_store8) [0x64e677081bdf]
/media/test/ruby/build/ruby(st_general_foreach+0x12e4) [0x64e677315414] /media/test/ruby/build/./st.c:1560
/media/test/ruby/build/ruby(rb_hash_stlike_foreach_with_replace+0x16) [0x64e677133dcf] /media/test/ruby/build/./hash.c:1425
/media/test/ruby/build/ruby(rb_hash_transform_values_bang) /media/test/ruby/build/./hash.c:3552
/media/test/ruby/build/ruby(vm_cfp_consistent_p+0x0) [0x64e67745a9dc] ../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) [0x64e67744304b] ../vm_insnhelper.c:4776
./ruby(vm_call_method+0x2d4) [0x64e677442b14]
/media/test/ruby/build/ruby(vm_sendish+0x11f) [0x64e67740a53a] ../vm_insnhelper.c:5995
/media/test/ruby/build/ruby(vm_exec_core) ../insns.def:851
./ruby(vm_exec_loop+0x0) [0x64e6773ffcd8]
/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) [0x64e6770bbb1] /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) [0x64e6770b72b1] /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) [0x7c2903e2a1ca] ../sysdeps/nptl/libc_start_call_main.h:58
/lib/x86_64-linux-gnu/libc.so.6(call_init+0x0) [0x7c2903e2a28b] ../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) [0x64e676fddd95]

-- Other runtime information -----

* Loaded script: triaged/hash_transform_values.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 [bb180b87](#) - 05/13/2025 02:16 PM - nobu (Nobuyoshi Nakada)

[Bug #21331] Prohibit modification during stlike loop

Revision 862480a3 - 05/14/2025 12:14 AM - k0kubun (Takashi Kokubun)

merge revision(s) bb180b87b43c45e17ff49735a26d7a188d5c8396: [Backport #21331]

```
[Bug #21331] Prohibit modification during stlike loop
```

Revision b66c5c3b - 05/14/2025 01:23 AM - nobu (Nobuyoshi Nakada)

Revert "[Bug #21331] Prohibit modification during stlike loop"

This reverts commit bb180b87b43c45e17ff49735a26d7a188d5c8396, which caused "malloc during GC" error on wasm.

Revision 7793b59c - 05/14/2025 01:37 AM - nobu (Nobuyoshi Nakada)

[Bug #21331] Prohibit hash modification during stlike loop

Revision fbc3271 - 05/14/2025 03:00 AM - nobu (Nobuyoshi Nakada)

Revert "[Bug #21331] Prohibit modification during stlike loop"

This reverts commit bb180b87b43c45e17ff49735a26d7a188d5c8396, which caused "malloc during GC" error on wasm.

Revision a21b88a6 - 05/14/2025 03:01 AM - nobu (Nobuyoshi Nakada)

[Bug #21331] Prohibit hash modification during stlike loop

Revision cb49400d - 05/17/2025 06:57 AM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 7793b59c8d2a13c124fe276e11723db23facce04: [Backport #21331]

```
[Bug #21331] Prohibit hash modification during stlike loop
```

History

#1 - 05/13/2025 01:49 PM - nobu (Nobuyoshi Nakada)

- Backport changed from 3.2: UNKNOWN, 3.3: UNKNOWN, 3.4: UNKNOWN to 3.2: REQUIRED, 3.3: REQUIRED, 3.4: REQUIRED

#2 - 05/13/2025 01:49 PM - nobu (Nobuyoshi Nakada)

<https://github.com/ruby/ruby/pull/13317>

#3 - 05/13/2025 04:37 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset [git|bb180b87b43c45e17ff49735a26d7a188d5c8396](https://github.com/ruby/ruby/commit/bb180b87b43c45e17ff49735a26d7a188d5c8396).

[Bug [#21331](#)] Prohibit modification during stlike loop

#4 - 05/14/2025 12:15 AM - k0kubun (Takashi Kokubun)

- Backport changed from 3.2: REQUIRED, 3.3: REQUIRED, 3.4: REQUIRED to 3.2: REQUIRED, 3.3: REQUIRED, 3.4: DONE

ruby_3_4 [862480a316c014d2b4659b22cd12e311c0810105](#) merged revision(s) [bb180b87b43c45e17ff49735a26d7a188d5c8396](#).

#5 - 05/14/2025 06:20 AM - byroot (Jean Boussier)

[@nobu \(Nobuyoshi Nakada\)](#) given you reverted your fix, should we re-open?

#6 - 05/17/2025 07:44 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 3.2: REQUIRED, 3.3: REQUIRED, 3.4: DONE to 3.2: REQUIRED, 3.3: DONE, 3.4: DONE

ruby_3_3 [cb49400d680894d69534b0b4cd10b085de325e2a](#) merged revision(s) [7793b59c8d2a13c124fe276e11723db23facce04](#).