

Ruby - Bug #15122

Segfault when marshaling an IO object

09/14/2018 05:07 PM - larskanis (Lars Kanis)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.6.0dev (2018-09-13 trunk 64736) [x86_64-linux]	Backport: 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN

Description

When I run:

```
$ ruby -e "Marshal.dump(IO.pipe[1])"
```

Expected behavior:

I would expect a TypeError

Actual behavior:

I get a Segfault:

```
-e:1: [BUG] Segmentation fault at 0x0000000000000020
ruby 2.6.0dev (2018-08-26 trunk 64542) [x86_64-linux]

-- Control frame information -----
c:0003 p:---- s:0011 e:000010 CFUNC :dump
c:0002 p:0024 s:0006 e:000005 EVAL -e:1 [FINISH]
c:0001 p:0000 s:0003 E:000610 (none) [FINISH]

-- Ruby level backtrace information -----
-e:1:in `<main>'
-e:1:in `dump'

-- Machine register context -----
RIP: 0x00007fe2347a2a5e RBP: 0x0000561904cc2798 RSP: 0x00007fff047e2840
RAX: 0x0000000000000008 RBX: 0x0000561904ccec78 RCX: 0x0000000000000000
RDX: 0x00007fe234e32f68 RDI: 0x0000000000000000 RSI: 0x0000561904ccec78
R8: 0x0000000000000000 R9: 0x00005619048e07d8 R10: 0x0000000000000000
R11: 0x0000000000000000 R12: 0x0000561904ccec00 R13: 0x0000561904cc2770
R14: 0x0000000000000000 R15: 0x00000000ffffffff EFL: 0x0000000000010202

-- C level backtrace information -----
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(rb_vm_bugreport+0x769) [0x7fe23495b719] vm_dump.c:704
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(rb_bug_context+0xd4) [0x7fe2347b9114] error.c:610
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(sigsegv+0x42) [0x7fe2348caba2] signal.c:980
/lib/x86_64-linux-gnu/libc.so.6(0x7fe234353f20) [0x7fe234353f20]
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(rb_enc_get_index+0x8e) [0x7fe2347a2a5e] encoding.c:803
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(encoding_name.isra.18+0x24) [0x7fe23480d504] marshal.c:582
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(w_object+0x522) [0x7fe234811682] marshal.c:772
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(marshal_dump+0x1ce) [0x7fe2348137de] marshal.c:1057
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(vm_call_cfunc+0xea) [0x7fe23493d9ca] vm_insnhelper.c:1932
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(vm_call_method+0xd3) [0x7fe23494f293] vm_insnhelper.c:2422
```

```
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(vm_exec_core+0x128) [0x7fe234946688] /home/lars/.rvm/src/ruby-head/insns.def:774
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(rb_vm_exec+0x9c) [0x7fe23494cb3c] vm.c:1810
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(ruby_exec_internal+0xc4) [0x7fe2347bfc74] eval.c:261
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(ruby_exec_node+0x1d) [0x7fe2347c1ced] eval.c:325
/home/lars/.rvm/rubies/ruby-head/lib/libruby.so.2.6(ruby_run_node+0x1e) [0x7fe2347c551e] eval.c:317
/home/lars/.rvm/rubies/ruby-head/bin/ruby(main+0x5f) [0x561902d1099f] ./main.c:42
```

Affected ruby versions

Only ruby-head

Additional info

I got this segfault when testing the [eventbox gem](#) on ruby-head: <https://travis-ci.com/larskanis/eventbox/jobs/145817878>

Associated revisions

Revision e04046515389ba4d019a13db33de198b85480b00 - 09/15/2018 04:27 PM - nobu (Nobuyoshi Nakada)

encoding.c: check external encoding

- encoding.c (rb_enc_get_index): external encoding may not be Data object. [ruby-core:89016] [Bug #15122]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64753 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e04046515389ba4d019a13db33de198b85480b00 - 09/15/2018 04:27 PM - nobu (Nobuyoshi Nakada)

encoding.c: check external encoding

- encoding.c (rb_enc_get_index): external encoding may not be Data object. [ruby-core:89016] [Bug #15122]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64753 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision e0404651 - 09/15/2018 04:27 PM - nobu (Nobuyoshi Nakada)

encoding.c: check external encoding

- encoding.c (rb_enc_get_index): external encoding may not be Data object. [ruby-core:89016] [Bug #15122]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@64753 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 09/14/2018 10:36 PM - wanabe (_ wanabe)

git bisect shows this is from

<https://bugs.ruby-lang.org/projects/ruby-trunk/repository/ruby-git/revisions/a2c7d0cea999bc8f8e6deb89bcee5eb80ba13ea2> = r64178.

I guess pipe IO doesn't have internal_encoding nor external_encoding.

#2 - 09/15/2018 04:27 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset trunk|r64753.

encoding.c: check external encoding

- encoding.c (rb_enc_get_index): external encoding may not be Data object. [ruby-core:89016] [Bug #15122]