

Ruby - Bug #20903

Segmentation fault when string encoding

11/21/2024 01:14 PM - bendrissou (Bachir Bendrissou)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	3.3.5	Backport: 3.1: UNKNOWN, 3.2: UNKNOWN, 3.3: UNKNOWN

Description

I am getting a segmentation fault. The error appears to relate to the string encoding function: rb_enc_str_coderange.

Test case:

```
require 'test/unit'
require "-test-/econv"

class Test_EConvAppend < Test::Unit::TestCase

  def test_econv_str_append_valid
    ec=Bug::EConv.new("utf-8", "cp932")
    ret=ec.append("\u3042"*30,5)
  end

end
```

Output:

```
test.rb:8: [BUG] Segmentation fault at 0x000000000000000b
ruby 3.3.5 (2024-09-03 revision ef084cc8f4) [x86_64-linux]

-- Control frame information -----
c:0026 p:---- s:0152 e:000151 CFUNC :append
c:0025 p:0022 s:0146 e:000145 METHOD test.rb:8
c:0024 p:0037 s:0140 e:000139 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit/testcase.rb:202
c:0023 p:0052 s:0134 e:000133 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit/testcase.rb:170
c:0022 p:0083 s:0125 e:000124 BLOCK /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1552 [FINISH]
c:0021 p:---- s:0118 e:000117 CFUNC :map
c:0020 p:0103 s:0114 e:000113 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1539
c:0019 p:0035 s:0102 e:000101 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1332
c:0018 p:0010 s:0095 e:000093 BLOCK /home/benchmarks/ruby/program/tool/lib/test/unit.rb:793 [FINISH]
c:0017 p:---- s:0089 e:000088 CFUNC :each
c:0016 p:0047 s:0085 e:000084 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:791
c:0015 p:0008 s:0078 e:000077 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:828
c:0014 p:0127 s:0071 e:000070 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1485
c:0013 p:0016 s:0058 e:000057 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1269
c:0012 p:0005 s:0053 e:000052 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1660
c:0011 p:0006 s:0049 e:000048 BLOCK /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1647 [FINISH]
c:0010 p:---- s:0045 e:000044 CFUNC :each
c:0009 p:0042 s:0041 e:000040 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1646
c:0008 p:0013 s:0036 e:000035 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1689
c:0007 p:0008 s:0031 e:000030 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1016
c:0006 p:0008 s:0025 e:000024 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:861
c:0005 p:0017 s:0019 e:000018 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:125
c:0004 p:0009 s:0014 e:000012 BLOCK /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1700
c:0003 p:0015 s:0010 e:000009 METHOD /home/benchmarks/ruby/program/tool/lib/test/unit.rb:131
```

```

c:0002 p:0013 s:0006 e:000005 BLOCK /home/benchmarks/ruby/program/tool/lib/test/unit.rb:1699 [FINISH]
c:0001 p:0000 s:0003 E:0026f0 DUMMY [FINISH]

-- Ruby level backtrace information -----
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1699:in `block in autorun'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:131:in `run_once'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1700:in `block (2 levels) in autorun'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:125:in `run'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:861:in `run'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1016:in `run'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1689:in `run'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1646:in `_run'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1646:in `each'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1647:in `block in _run'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1660:in `run_tests'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1269:in `_run_anything'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1485:in `_run_anything'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:828:in `_run_suites'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:791:in `_run_suites'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:791:in `each'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:793:in `block in _run_suites'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1332:in `_run_suite'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1539:in `_run_suite'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1539:in `map'
/home/benchmarks/ruby/program/tool/lib/test/unit.rb:1552:in `block in _run_suite'
/home/benchmarks/ruby/program/tool/lib/test/unit/testcase.rb:170:in `run'
/home/benchmarks/ruby/program/tool/lib/test/unit/testcase.rb:202:in `run_test'
test.rb:8:in `test_econv_str_append_valid'
test.rb:8:in `append'

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

-- Machine register context -----
RIP: 0x0000564c868ae504 RBP: 0x0000564c87e51bc0 RSP: 0x00007ffd6b628e68
RAX: 0x0000000000000000 RBX: 0x000000000000005a RCX: 0x000000000000000b
RDX: 0x000000000000005a RDI: 0x000000000000000b RSI: 0x00007f35092de3a8
R8: 0x0000000000000000 R9: 0x000000000000001f R10: 0x00007f35093d448d
R11: 0x0000564c868fe070 R12: 0x00007f35092de3a8 R13: 0x000000000000005a
R14: 0x0000564c87e51bc0 R15: 0x000000000000000b EFL: 0x0000000000010202

-- C level backtrace information -----
/home/benchmarks/ruby/program/build/ruby(rb_print_backtrace+0x11) [0x564c8694aa7f] ../vm_dump.c:820
/home/benchmarks/ruby/program/build/ruby(rb_vm_bugreport) ../vm_dump.c:1151
/home/benchmarks/ruby/program/build/ruby(rb_bug_for_fatal_signal+0xfc) [0x564c86b16a6c] ../error.c:1065
/home/benchmarks/ruby/program/build/ruby(sigsegv+0x4d) [0x564c868991fd] ../signal.c:926
/lib/x86_64-linux-gnu/libpthread.so.0(__restore_rt+0x0) [0x7f3524817420]
/home/benchmarks/ruby/program/build/ruby(RB_FL_TEST_RAW+0x0) [0x564c868ae504] ../string.c:770
/home/benchmarks/ruby/program/build/ruby(RB_ENC_CODERANGE) ../include/ruby/internal/encoding/coderange.h:97
/home/benchmarks/ruby/program/build/ruby(rb_enc_str_coderange) ../string.c:771
/home/benchmarks/ruby/program/build/ruby(rb_econv_append+0x52) [0x564c868fdde2] ../transcode.c:1865
/home/benchmarks/ruby/program/build/ruby(rb_econv_substr_append+0x22) [0x564c868fe0ce] ../transcode.c:1913
/home/benchmarks/ruby/program/build/ruby(rb_econv_str_append) ../transcode.c:1921
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame+0x7b) [0x564c8691db06] ../vm_insnhelper.c:3502
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame) ../vm_insnhelper.c:3530
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_other) ../vm_insnhelper.c:3556
/home/benchmarks/ruby/program/build/ruby(vm_call_method_each_type+0x81) [0x564c8692d691] ../vm_insnhelper.c:4429
/home/benchmarks/ruby/program/build/ruby(vm_call_method+0xc4) [0x564c8692e374] ../vm_insnhelper.c:

```

```
4581
/home/benchmarks/ruby/program/build/ruby(vm_sendish+0xe) [0x564c8693b19f] ../vm_insnhelper.c:5593
/home/benchmarks/ruby/program/build/ruby(vm_exec_core) insns.def:834
/home/benchmarks/ruby/program/build/ruby(rb_vm_exec+0x18e) [0x564c8692c6be] ../vm.c:2486
/home/benchmarks/ruby/program/build/ruby(invoker_block_from_c_bh+0x2ca) [0x564c8693035a] ../vm.c:15
09
/home/benchmarks/ruby/program/build/ruby(rb_yield+0x70) [0x564c86930bc0] ../vm.c:1634
/home/benchmarks/ruby/program/build/ruby(RB_FL_TEST_RAW+0x0) [0x564c86a5f376] ../array.c:3633
/home/benchmarks/ruby/program/build/ruby(RB_FL_ANY_RAW) ../include/ruby/internal/fl_type.h:520
/home/benchmarks/ruby/program/build/ruby(rb_array_len) ../include/ruby/internal/core/rarray.h:259
/home/benchmarks/ruby/program/build/ruby(rb_ary_push) ../array.c:1340
/home/benchmarks/ruby/program/build/ruby(rb_ary_collect) ../array.c:3633
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame+0x78) [0x564c8691d795] ../vm_in
snhelper.c:3502
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame) ../vm_insnhelper.c:3530
/home/benchmarks/ruby/program/build/ruby(vm_sendish+0xe) [0x564c8693c4bf] ../vm_insnhelper.c:5593
/home/benchmarks/ruby/program/build/ruby(vm_exec_core) insns.def:814
/home/benchmarks/ruby/program/build/ruby(rb_vm_exec+0x18e) [0x564c8692c6be] ../vm.c:2486
/home/benchmarks/ruby/program/build/ruby(invoker_block_from_c_bh+0x2ca) [0x564c8693035a] ../vm.c:15
09
/home/benchmarks/ruby/program/build/ruby(rb_yield+0x70) [0x564c86930bc0] ../vm.c:1634
/home/benchmarks/ruby/program/build/ruby(RB_FL_TEST_RAW+0x0) [0x564c86a5973c] ../array.c:2538
/home/benchmarks/ruby/program/build/ruby(RB_FL_ANY_RAW) ../include/ruby/internal/fl_type.h:520
/home/benchmarks/ruby/program/build/ruby(rb_array_len) ../include/ruby/internal/core/rarray.h:259
/home/benchmarks/ruby/program/build/ruby(rb_ary_each) ../array.c:2537
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame+0x78) [0x564c8691d795] ../vm_in
snhelper.c:3502
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame) ../vm_insnhelper.c:3530
/home/benchmarks/ruby/program/build/ruby(vm_sendish+0xe) [0x564c8693c4bf] ../vm_insnhelper.c:5593
/home/benchmarks/ruby/program/build/ruby(vm_exec_core) insns.def:814
/home/benchmarks/ruby/program/build/ruby(rb_vm_exec+0x18e) [0x564c8692c6be] ../vm.c:2486
/home/benchmarks/ruby/program/build/ruby(invoker_block_from_c_bh+0x2ca) [0x564c8693035a] ../vm.c:15
09
/home/benchmarks/ruby/program/build/ruby(rb_yield+0x70) [0x564c86930bc0] ../vm.c:1634
/home/benchmarks/ruby/program/build/ruby(RB_FL_TEST_RAW+0x0) [0x564c86a5973c] ../array.c:2538
/home/benchmarks/ruby/program/build/ruby(RB_FL_ANY_RAW) ../include/ruby/internal/fl_type.h:520
/home/benchmarks/ruby/program/build/ruby(rb_array_len) ../include/ruby/internal/core/rarray.h:259
/home/benchmarks/ruby/program/build/ruby(rb_ary_each) ../array.c:2537
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame+0x78) [0x564c8691d795] ../vm_in
snhelper.c:3502
/home/benchmarks/ruby/program/build/ruby(vm_call_cfunc_with_frame) ../vm_insnhelper.c:3530
/home/benchmarks/ruby/program/build/ruby(vm_sendish+0xe) [0x564c8693c4bf] ../vm_insnhelper.c:5593
/home/benchmarks/ruby/program/build/ruby(vm_exec_core) insns.def:814
/home/benchmarks/ruby/program/build/ruby(vm_exec_loop+0xa) [0x564c8692c937] ../vm.c:2513
/home/benchmarks/ruby/program/build/ruby(rb_vm_exec) ../vm.c:2492
/home/benchmarks/ruby/program/build/ruby(vm_invoke_proc+0x201) [0x564c86931421] ../vm.c:1509
/home/benchmarks/ruby/program/build/ruby(rb_vm_invoke_proc+0x33) [0x564c86931743] ../vm.c:1728
/home/benchmarks/ruby/program/build/ruby(rb_proc_call_kw+0x1a) [0x564c8682fcee] ../proc.c:957
/home/benchmarks/ruby/program/build/ruby(rb_proc_call) ../proc.c:967
/home/benchmarks/ruby/program/build/ruby(exec_end_procs_chain+0x43) [0x564c86740bfd] ../eval_jump.
c:105
/home/benchmarks/ruby/program/build/ruby(rb_ec_exec_end_proc) ../eval_jump.c:120
/home/benchmarks/ruby/program/build/ruby(rb_ec_teardown+0xd5) [0x564c86740e35] ../eval.c:159
/home/benchmarks/ruby/program/build/ruby(rb_ec_cleanup+0x152) [0x564c86741042] ../eval.c:212
/home/benchmarks/ruby/program/build/ruby(ruby_run_node+0x59) [0x564c86741a29] ../eval.c:328
/home/benchmarks/ruby/program/build/ruby(rb_main+0x21) [0x564c8673c437] ../main.c:39
/home/benchmarks/ruby/program/build/ruby(main) ../main.c:58
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf3) [0x7f3524618083]
[0x564c8673c48e]
```

Associated revisions

Revision 4e01878badf6bbc06fa6538f6bea199f772b1b3e - 11/22/2024 01:36 AM - nobu (Nobuyoshi Nakada)

[Bug #20903] rb_econv_str_append arguments expected to be String

Revision 4e01878badf6bbc06fa6538f6bea199f772b1b3e - 11/22/2024 01:36 AM - nobu (Nobuyoshi Nakada)

[Bug #20903] rb_econv_str_append arguments expected to be String

Revision 4e01878b - 11/22/2024 01:36 AM - nobu (Nobuyoshi Nakada)

[Bug #20903] rb_econv_str_append arguments expected to be String

History

#1 - 11/22/2024 02:42 AM - nobu (Nobuyoshi Nakada)

Thank you, I've forgotten to add the test case using it. There is test/-ext-/econv/test_append.rb.
<https://github.com/ruby/ruby/pull/12145>

#2 - 11/22/2024 03:25 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset [git|4e01878badf6bbc06fa6538f6bea199f772b1b3e](https://github.com/ruby/ruby/pull/12145).

[Bug [#20903](#)] rb_econv_str_append arguments expected to be String