

Ruby - Bug #14660

RubyVM::InstructionSequence.load_from_binary(bin).eval may cause SEGV after r62856

04/02/2018 11:50 PM - wanabe (_ wanabe)

Status:	Closed	Backport: 2.3: UNKNOWN, 2.4: UNKNOWN, 2.5: UNKNOWN
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		
Description		
A certain script can cause SEGV when ISeq#to_binary -> load_from_binary -> eval.		
<pre>\$./miniruby -ve 'str = "class P; def p; end; def q; end; E = \"\"; N = \"#{E}\"; attr_reader :i; end"; iseq = RubyVM::InstructionSequence.compile(str); bin = iseq.to_binary; RubyVM::InstructionSequence.load_from_binary(bin).eval' ruby 2.6.0dev (2018-04-02 trunk 63063) [x86_64-linux] Segmentation fault (core dumped)</pre>		
(Note above script is shortened version of "minitest/pride_plugin.rb")		
git bisect shows it is since r62856, but I don't know the commit is "bad" or not. It may make apparent a hidden bug, or increase the probability of reproduction.		

Associated revisions

Revision 02df45c4c42e21f7e84221f8202fc8ea4ff25805 - 04/03/2018 10:50 AM - nobu (Nobuyoshi Nakada)

Reproducible test for [Feature#14370] @ [Bug #14660]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@63075 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 02df45c4 - 04/03/2018 10:50 AM - nobu (Nobuyoshi Nakada)

Reproducible test for [Feature#14370] @ [Bug #14660]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@63075 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7084c015bf09fbe1687f51953fce0f96fc48dab9 - 04/05/2018 01:13 PM - nobu (Nobuyoshi Nakada)

compile.c: fix positions encode

- compile.c (ibf_load_iseq_each): iseq_size necessary to encode positions is set in ibf_load_code(). [Bug #14660]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@63103 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7084c015 - 04/05/2018 01:13 PM - nobu (Nobuyoshi Nakada)

compile.c: fix positions encode

- compile.c (ibf_load_iseq_each): iseq_size necessary to encode positions is set in ibf_load_code(). [Bug #14660]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@63103 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 04/03/2018 07:57 AM - nobu (Nobuyoshi Nakada)

It's since r62851.

#2 - 04/03/2018 10:50 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

Applied in changeset trunk|r63075.

Reproducible test for [Feature#14370] @ [Bug [#14660](#)]

#3 - 04/03/2018 11:32 AM - nobu (Nobuyoshi Nakada)

- *Status changed from Closed to Open*

It's probably a bug of IBF, and has been revealed by [Feature#14370], I guess.

#4 - 04/05/2018 01:13 PM - nobu (Nobuyoshi Nakada)

- *Status changed from Open to Closed*

Applied in changeset trunk|r63103.

compile.c: fix positions encode

- compile.c (ibf_load_isseq_each): iseq_size necessary to encode positions is set in ibf_load_code(). [Bug [#14660](#)]