Ruby master - Bug #11851

**rb_profile_frames() causes segmentation fault**

12/20/2015 08:58 AM - rhenium (Kazuki Yamaguchi)

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td></td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>ruby -v:</td>
<td>ruby 2.3.0dev (2015-12-20 trunk 53215) [x86_64-linux]</td>
</tr>
</tbody>
</table>

**Description**

When the control frame stack contains an ifunc-frame, calling rb_profile_frames() causes a segmentation fault.

I've attached a patch that changes it to ignore ifunc frames as it did previously.

**Associated revisions**

Revision cc52f511 - 12/21/2015 01:18 AM - nobu (Nobuyoshi Nakada)

vm_backtrace.c: ignore ifunc frames

- vm_backtrace.c (rb_profile_frames): ignore ifunc frames as it did before. [ruby-core:72409] [Bug #11851]

  git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@53225 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 53225 - 12/21/2015 01:18 AM - nobu (Nobuyoshi Nakada)

vm_backtrace.c: ignore ifunc frames

- vm_backtrace.c (rb_profile_frames): ignore ifunc frames as it did before. [ruby-core:72409] [Bug #11851]

Revision 53225 - 12/21/2015 01:18 AM - nobu (Nobuyoshi Nakada)

vm_backtrace.c: ignore ifunc frames

- vm_backtrace.c (rb_profile_frames): ignore ifunc frames as it did before. [ruby-core:72409] [Bug #11851]

Revision 53225 - 12/21/2015 01:18 AM - nobu (Nobuyoshi Nakada)

vm_backtrace.c: ignore ifunc frames

- vm_backtrace.c (rb_profile_frames): ignore ifunc frames as it did before. [ruby-core:72409] [Bug #11851]

Revision 53225 - 12/21/2015 01:18 AM - nobu (Nobuyoshi Nakada)

vm_backtrace.c: ignore ifunc frames

- vm_backtrace.c (rb_profile_frames): ignore ifunc frames as it did before. [ruby-core:72409] [Bug #11851]

Revision 53225 - 12/21/2015 01:18 AM - nobu (Nobuyoshi Nakada)

vm_backtrace.c: ignore ifunc frames

- vm_backtrace.c (rb_profile_frames): ignore ifunc frames as it did before. [ruby-core:72409] [Bug #11851]

**History**

#1 - 12/20/2015 11:48 AM - nobu (Nobuyoshi Nakada)

Could you show reproducible code or add a test?

#2 - 12/20/2015 12:57 PM - rhenium (Kazuki Yamaguchi)

Uploaded reproducible code to Gist: [https://gist.github.com/rhenium/e3a179b0cac87606c183](https://gist.github.com/rhenium/e3a179b0cac87606c183)

This runs on Ruby 2.2.4 and patched trunk but segfaults on trunk.

#3 - 12/21/2015 01:19 AM - nobu (Nobuyoshi Nakada)
- Status changed from Open to Closed

Applied in changeset r53225.

vm_backtrace.c: ignore ifunc frames

- vm_backtrace.c (rb_profile_frames): ignore ifunc frames as it did before. [ruby-core:72409] [Bug #11851]

#4 - 02/03/2016 10:37 AM - usa (Usaku NAKAMURA)
- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.0.0: DONTNEED, 2.1: DONTNEED, 2.2: DONTNEED

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001-vm_backtrace.c-rb_profile_frames-ignore-ifunc-frames.patch</td>
<td>1.36 KB</td>
<td>12/20/2015</td>
<td>rhenium (Kazuki Yamaguchi)</td>
</tr>
</tbody>
</table>