

r25230 causes SEGV around Marshal

11/20/2009 07:54 AM - naruse (Yui NARUSE)

Status: Closed Priority: Normal Assignee: nobu (Nobuyoshi Nakada) Target version: 1.9.2 ruby -v: ruby 1.9.2dev (2009-11-19 trunk 25848) [i686-linux]	Backport:
--	------------------

[illegible]

Author: nobu nobu@b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Date: Sun Oct 4 10:30:56 2009 +0000

```
* marshal.c (struct {dump,load}_arg): manage with dfree, instead
of using local variable which may be moved by context switch.
[ruby-dev:39425]
```

<http://svn.ruby-lang.org/cgi-bin/viewvc.cgi?view=rev&revision=25230>

□□□□□□□□□□.

```
ruby
#####
#####?
```

```
% ruby -v
ruby 1.9.2dev (2009-11-19 trunk 25848) [i686-linux]
```

each: method `to_s' called on hidden object (0x9438e48)

```
00, 00000000: 000000 SEGV000000000000
000... 000, 000000000?
```

ruby

```
/usr/local/apps/rubyware/ruby-1.9.2-20091118/lib/ruby/1.9.1/delegate.rb:265: [BUG] Segmentation fault
ruby 1.9.2dev (2009-11-18 trunk 25846) [i686-linux]
```

```
-- control frame -----
```

```
c:0037 p:---- s:0130 b:0130 l:000129 d:000129 CFUNC :write
c:0036 p:0026 s:0126 b:0126 l:000768 d:000125 LAMBDA
/usr/local/apps/rubyware/ruby-1.9.2-20091118/lib/ruby/1.9.1/delegate.rb:265
c:0035 p:---- s:0121 b:0121 l:000120 d:000120 FINISH
c:0034 p:---- s:0119 b:0119 l:000118 d:000118 CFUNC :dump
c:0033 p:0062 s:0114 b:0114 l:000ba8 d:000113 BLOCK
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:863
c:0032 p:0050 s:0110 b:0110 l:000109 d:000109 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:849
c:0031 p:0011 s:0105 b:0105 l:000ba8 d:000ba8 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:859
c:0030 p:0079 s:0101 b:0101 l:000095 d:000100 BLOCK
```

/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:787
c:0029 p:0019 s:0099 b:0099 l:000098 d:000098 METHOD [internal:prelude:8](#)
c:0028 p:0013 s:0096 b:0096 l:000095 d:000095 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:780
c:0027 p:0015 s:0092 b:0092 l:000091 d:000091 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:303
c:0026 p:0118 s:0088 b:0088 l:001e8c d:000087 BLOCK
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/n-group-by.rb:56
c:0025 p:---- s:0083 b:0083 l:000082 d:000082 FINISH
c:0024 p:---- s:0081 b:0081 l:000080 d:000080 CFUNC :call
c:0023 p:0014 s:0077 b:0077 l:0011ec d:000076 BLOCK test/testc.rb:3196
c:0022 p:---- s:0074 b:0074 l:000073 d:000073 FINISH
c:0021 p:---- s:0072 b:0072 l:000071 d:000071 CFUNC :each
c:0020 p:0032 s:0069 b:0069 l:0011ec d:00263c BLOCK test/testc.rb:3195
c:0019 p:---- s:0065 b:0065 l:000064 d:000064 FINISH
c:0018 p:---- s:0063 b:0063 l:000062 d:000062 CFUNC :each
c:0017 p:0017 s:0060 b:0060 l:000059 d:000059 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/nfile.rb:78
c:0016 p:0073 s:0056 b:0056 l:000055 d:000055 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:156
c:0015 p:0011 s:0051 b:0051 l:0011ec d:00074c BLOCK test/testc.rb:3188
c:0014 p:---- s:0047 b:0047 l:000046 d:000046 FINISH
c:0013 p:---- s:0045 b:0045 l:000044 d:000044 CFUNC :yield
c:0012 p:0014 s:0040 b:0040 l:0000dc d:000039 BLOCK
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/share/block-source.rb:81
c:0011 p:0021 s:0038 b:0038 l:000037 d:000037 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/share/stdout.rb:35
c:0010 p:0014 s:0034 b:0034 l:0000dc d:0000dc METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/share/block-source.rb:80
c:0009 p:0043 s:0029 b:0029 l:000028 d:000028 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/n-each-substream-mapper.r
b:26
c:0008 p:0073 s:0025 b:0025 l:000024 d:000024 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:156
c:0007 p:0137 s:0020 b:0020 l:001e8c d:001f2c BLOCK
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/n-group-by.rb:47
c:0006 p:---- s:0016 b:0016 l:000015 d:000015 FINISH
c:0005 p:---- s:0014 b:0014 l:000013 d:000013 CFUNC :call
c:0004 p:0012 s:0011 b:0011 l:000010 d:000010 METHOD
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:143
c:0003 p:0077 s:0007 b:0007 l:0020f8 d:000006 BLOCK
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:125
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:---- s:0002 b:0002 l:000001 d:000001 TOP

/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:125:in block in start'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:143:in basic_start'

```
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:143:in call'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/n-group-by.rb:47:in block in start_export'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:156:in each'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/n-each-substream-mapper.rb:26:in basic_each'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/share/block-source.rb:80:in yield19'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/share/stdout.rb:35:in replace_stdout'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/share/block-source.rb:81:in block in yield19'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/share/block-source.rb:81:in yield'
test/testc.rb:3188:in block in context' /home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/njob.rb:156:in each'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/nfile.rb:78:in basic_each'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/nfile.rb:78:in each'
test/testc.rb:3195:in block (2 levels) in context' test/testc.rb:3195:in each'
test/testc.rb:3196:in block (3 levels) in context' test/testc.rb:3196:in call'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/n-group-by.rb:56:in block (2 levels) in start_export'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:303:in push'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:780:in push' <internal:prelude>:8:in synchronize'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:787:in block in push'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:859:in store_2ndmemory'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:849:in open_2ndmemory'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:863:in block in store_2ndmemory'
/home/keiju/public/a.research/fairy/git/fairy/lib/fairy/node/port.rb:863:in dump'
/usr/local/apps/rubyware/ruby-1.9.2-20091118/lib/ruby/1.9.1/delegate.rb:265:in block in delegating_block'
/usr/local/apps/rubyware/ruby-1.9.2-20091118/lib/ruby/1.9.1/delegate.rb:265:in `write'
```

-- C level backtrace information -----

```
fairy processor --node 45566 --id 0(rb_vm_bugreport+0xb5) [0x81621a5]
fairy processor --node 45566 --id 0 [0x819f3ce]
fairy processor --node 45566 --id 0(rb_bug+0x28) [0x819f468]
fairy processor --node 45566 --id 0 [0x80f71e5]
[0xb801c40c]
fairy processor --node 45566 --id 0(rb_funcall+0xe1) [0x815ee81]
fairy processor --node 45566 --id 0(rb_obj_as_string+0x81) [0x8103811]
fairy processor --node 45566 --id 0 [0x8079378]
fairy processor --node 45566 --id 0 [0x8151689]
fairy processor --node 45566 --id 0 [0x8152bbd]
fairy processor --node 45566 --id 0 [0x815511d]
fairy processor --node 45566 --id 0 [0x8159399]
fairy processor --node 45566 --id 0(rb_vm_invoke_proc+0x81) [0x8159b61]
fairy processor --node 45566 --id 0 [0x815aab5]
fairy processor --node 45566 --id 0(rb_funcall+0x18e) [0x815ef2e]
fairy processor --node 45566 --id 0(rb_io_write+0x29) [0x80712a9]
fairy processor --node 45566 --id 0 [0x8089f38]
fairy processor --node 45566 --id 0 [0x814d71d]
fairy processor --node 45566 --id 0 [0x8151689]
fairy processor --node 45566 --id 0 [0x8152bbd]
fairy processor --node 45566 --id 0 [0x815511d]
fairy processor --node 45566 --id 0 [0x8159399]
fairy processor --node 45566 --id 0(rb_vm_invoke_proc+0x81) [0x8159b61]
fairy processor --node 45566 --id 0 [0x8062ec4]
fairy processor --node 45566 --id 0 [0x814d71d]
fairy processor --node 45566 --id 0 [0x8151689]
fairy processor --node 45566 --id 0 [0x8152bbd]
fairy processor --node 45566 --id 0 [0x815511d]
fairy processor --node 45566 --id 0 [0x8159399]
fairy processor --node 45566 --id 0(rb_yield+0x4f) [0x816103f]
fairy processor --node 45566 --id 0(rb_ary_each+0x41) [0x81716a1]
fairy processor --node 45566 --id 0 [0x8151689]
fairy processor --node 45566 --id 0 [0x8152bbd]
fairy processor --node 45566 --id 0 [0x815511d]
fairy processor --node 45566 --id 0 [0x8159399]
fairy processor --node 45566 --id 0(rb_yield+0x4f) [0x816103f]
fairy processor --node 45566 --id 0 [0x8082bf8]
fairy processor --node 45566 --id 0 [0x814d71d]
fairy processor --node 45566 --id 0 [0x8151689]
fairy processor --node 45566 --id 0 [0x8152bbd]
fairy processor --node 45566 --id 0 [0x815511d]
fairy processor --node 45566 --id 0 [0x8159399]
```

Related issues:		
Related to Ruby - Bug #2390: Marshal.dump pass a hidden object	Closed	11/20/2009
Related to Ruby - Bug #3463: 1.9.2-preview3 [BUG] gc_sweep(): unknown data ...	Closed	06/22/2010

- Category set to core
- Status changed from Open to Assigned
- Assignee set to nobu (Nobuyoshi Nakada)
- Priority changed from 3 to Normal
- Target version set to 1.9.2
- ruby -v set to ruby 1.9.2dev (2009-11-19 trunk 25848) [i686-linux]

```
=end
```

```
=begin
```

```
-- marshal.c (revision 25922)
+++ marshal.c (working copy)
@@ -166,6 +166,7 @@ @@
return;
rb_mark_set(p->data);
rb_mark_hash(p->compat tbl);
```

- ```
static void
=end
```

```
=begin
□□□□□
```

~~~~~

Index: marshal.c

```
--- marshal.c (revision 25922)
+++ marshal.c (working copy)
@@ -166,6 +166,7 @@
return;
rb_mark_set(p->data);
rb_mark_hash(p->compat_tbl);
```

- rb\_gc\_mark(p->str);
}

static void

~~~~~

~~~~~ marshal\_dump ~~~~ GC ~~~~~~

```
diff --git a/marshal.c b/marshal.c
index 7acc495..cd747b8 100644
--- a/marshal.c
+++ b/marshal.c
@@ -941,6 +941,7 @@ marshal_dump(int argc, VALUE *argv)
port = arg->str;
}
```

- rb\_gc();
w\_byte(MARSHAL\_MAJOR, arg);
w\_byte(MARSHAL\_MINOR, arg);

~~~~~ SEGV ~~~~~~

```
$./miniruby -e '
class C
def marshal_dump
GC.start
""
end
end
o = Object.new
def o.write(s)
s
end
Marshal.dump(C.new, o)
'
-e:4: [BUG] rb_gc_mark(): unknown data type 0x0(0x8248bac) corrupted object
(snip)
```

--
Yusuke ENDOH [mame@tsg.ne.jp](mailto:mame@tsg.ne.jp)

=end

#4 - 11/26/2009 12:46 AM - matz (Yukihiro Matsumoto)

=begin
~~~~~

In message "Re: [\[ruby-dev:39774\]](#) [Bug [#2386](#)] r25230 causes SEGV around Marshal"
on Wed, 25 Nov 2009 23:08:16 +0900, \_ wanabe [redmine@ruby-lang.org](mailto:redmine@ruby-lang.org) writes:

```
|~~~~~
|
|Index: marshal.c
|=====
|--- marshal.c (revision 25922)
|+++ marshal.c (working copy)
```

000000000000

=end

#### #5 - 11/26/2009 04:43 AM - keiju (Keiju Ishitsuka)

=begin  
000000000000.

000000000000.

In [\[ruby-dev:39774\]](#) the message: "[[ruby-dev:39774](#)] [Bug [#2386](#)] r25230 causes SEGV around Marshal", on Nov/25 23:08(JST) \_ wanabe writes:

0000 [#2386](#) 0000000000 (by \_ wanabe)

000000000000000000000000000000000000

SEGV00000000000000. 0000000:

[P]#7 njob.rb[172] NFile#rescue in each: method to\_s' called on unexpected T\_NONE object (0x9bc8f64 flags=0x2000 klass=0x0)  
/usr/local/apps/rubyware/ruby-1.9.2-20091126/lib/ruby/1.9.1/delegate.rb:265:in write'  
/usr/local/apps/rubyware/ruby-1.9.2-20091126/lib/ruby/1.9.1/delegate.rb:265:in `block in delegating\_block'  
/

00000000000000. 0000000000000000...

00,

00000Marshal.dump(e, io) 0 ioTempfile000000000000  
000tempfile00000io000000000000000000dump0000000  
00000000000000000000

00000000, 00000, 00000000000000SEGV0000000000  
0(00000000000000). 000000, Tempfile00000000, 000  
0000000000, 000io00000000000010000000000000  
000000.

----->> 00 00 <-----  
----->> e-mail: [keiju@ishitsuka.com](mailto:keiju@ishitsuka.com) <-----

=end

#### #6 - 11/26/2009 07:37 AM - wanabe (\_ wanabe)

- Status changed from Assigned to Closed  
- % Done changed from 0 to 100

=begin  
This issue was solved with changeset r25927.  
Yui, thank you for reporting this issue.  
Your contribution to Ruby is greatly appreciated.  
May Ruby be with you.

=end

#### #7 - 11/26/2009 07:44 AM - wanabe (\_ wanabe)

- Status changed from Closed to Assigned

=begin  
0000000000000000000000000000  
=end

#### #8 - 04/27/2010 10:23 PM - mame (Yusuke Endoh)

- Status changed from Assigned to Feedback

=begin

```


#####
```

[illegible]

```
--
Yusuke Endoh mame@tsg.ne.jp
=end
```

**#9 - 04/28/2010 05:34 PM - keiju (Keiju Ishitsuka)**

```
=begin
□□□□□□□□□□□□.
```

In [\[ruby-dev:41080\]](#) the message: "[\[ruby-dev:41080\]](#) Bug #2386 r25230 causes SEGV around Marshal", on Apr/27 22:23(JST) Yusuke Endoh writes:

問題 #2386 問題文 (by Yusuke Endoh)  
 問題文 AssignedFeedback

□□□□□□□□□□□□□□□□□□□□

000. 0000000000000000000000...  
00000, 0000000000000000.

----->> 〇〇 〇〇 <<-----  
----->> e-mail: [keiju@ishitsuka.com](mailto:keiju@ishitsuka.com) <<-----

```
=end
```

**#10 - 04/28/2010 11:29 PM - mame (Yusuke Endoh)**

- Priority changed from Normal to 3

```
=begin
□□□□□
```

2010/4/28 17:33 送信先 [keiju@ishitsuka.com](mailto:keiju@ishitsuka.com):

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

000.00000000000000000000...  
0000, 000000000000.

10101010

Low

```
--
Yusuke Endoh mame@tsg.ne.jp
=end
```

**#11 - 06/11/2011 02:34 PM - ko1 (Koichi Sasada)**

- Status changed from Feedback to Closed

close