Hi,

tdiary's amazon.rb segfault in the cause of ruby's bug.

(tdiiary/lang/ja.rb):36:[BUG] Segmentation fault ruby 1.8.7 (2009-06-08 patchlevel 173) [i486-linux ]

It is reported to tdiary's BTS (in Japanese).

http://www.cozmixng.org/retro/projects/tdiary/tickets/142

It is investigated by hiraku, and his blog is in Japanese.

http://www.hinet.mydns.jp/tdiary/?date=20090506#p01
http://www.hinet.mydns.jp/tdiary/?date=20090508#p01

Here is simply reproduce one liner.

ruby -ve "C=0; o=''; o.instance_eval('def m; C; end'); o.clone.m"

And hiraku points that this bug is due to below patch.

debian/patches/905_class_dup_should_copy_constants.dpatch

It is introduced to ruby1.8 1.8.7.72-3 and dropped in ruby1.8 1.8.7.173-1 because of the upstream's inclusion.

This bug is fixed in ruby1.8 development branch.
But I do not know what revision fixes it... Sorry.

Regards,

dai

---

History

#1 - 08/12/2009 06:21 AM - akira (akira yamada)

=begin
(2009年06月19日 22:35), dai VDR さんは書きました:
Backport #1660: ruby1.8: tdiary's amazon.rb segfault in the cause of ruby's bug
http://redmine.ruby-lang.org/issues/show/1660

Forwarded from http://bugs.debian.org/533329

[...]

tdiary's amazon.rb segfault in the cause of ruby's bug.

(tdiiary/lang/ja.rb):36:[BUG] Segmentation fault ruby 1.8.7 (2009-06-08 patchlevel 173) [i486-linux ]

[...]

Here is simply reproduce one liner.

ruby -ve "C=0; o="; o.instance_eval("def m; C; end"); o.clone.m"

r22679ではないかなと思います。
とすると#1922 http://redmine.ruby-lang.org/issues/show/1922

--

#2 - 12/24/2009 04:21 PM - shyouhei (Shyouhei Urabe)
- Status changed from Open to Closed

=begin
This issue has already been fixed in the repository.
=end