Backport21 - Backport #9478
Fix segfault at unpacking modified String
02/04/2014 11:54 AM - nobu (Nobuyoshi Nakada)

Status: Closed
Priority: Normal
Assignee: naruse (Yui NARUSE)

Description
1.9でr44803で追加したテストがSEGVします。

Related issues:
- Related to Backport200 - Backport #9484: Fix segfault at unpacking modified String
  Closed 02/05/2014
- Related to Backport193 - Backport #9485: Fix segfault at unpacking modified String
  Closed 02/05/2014

Associated revisions
Revision 67345f7 - 02/05/2014 02:35 AM - naruse (Yui NARUSE)
merge revision(s) 44803: [Backport #9478]

* string.c (rb_str_modify_expand): enable capacity and disable association with packed objects when setting capa, so that pack("p") string fails to unpack properly after modified.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@44819 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 44819 - 02/05/2014 02:35 AM - naruse (Yui NARUSE)
merge revision(s) 44803: [Backport #9478]

* string.c (rb_str_modify_expand): enable capacity and disable association with packed objects when setting capa, so that pack("p") string fails to unpack properly after modified.

History
#1 - 02/04/2014 11:55 AM - nobu (Nobuyoshi Nakada)
- Tracker changed from Bug to Backport
- Project changed from Ruby master to Backport21

#2 - 02/05/2014 02:34 AM - nobu (Nobuyoshi Nakada)
- Assignee set to naruse (Yui NARUSE)

trunkではr44803で修正済みですが、1.9.3以降2.1まで（"\"].pack("p")<"a").unpack("p") でSEGVします。
1.9.2以降で問題ないようです。

#3 - 02/05/2014 02:35 AM - naruse (Yui NARUSE)
- Status changed from Open to Closed
- % Done changed from 0 to 100

Applied in changeset r44819.

merge revision(s) 44803: [Backport #9478]

* string.c (rb_str_modify_expand): enable capacity and disable association with packed objects when setting capa, so that pack("p") string fails to unpack properly after modified.

#4 - 02/05/2014 02:41 AM - nobu (Nobuyoshi Nakada)
- Related to Backport #9484: Fix segfault at unpacking modified String added

#5 - 02/05/2014 02:42 AM - nobu (Nobuyoshi Nakada)
- Related to Backport #9485: Fix segfault at unpacking modified String added