

Ruby - Bug #15934

String#b can lead to memory corruption

06/17/2019 07:50 PM - alanwu (Alan Wu)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	trunk(801d0d9), 2.4.6, 2.5.5, 2.6.3	Backport: 2.4: REQUIRED, 2.5: DONE, 2.6: DONE
Description The following script triggers use-after-free on trunk(801d0d9), 2.4.6, 2.5.5 and 2.6.3. <pre>a = ('j' * 24).b.b eval('', binding, a) p a 4.times { GC.start } p a</pre> The consequence is usually that a gets corrupted (it depends on what the system allocator does when it frees memory). Here is a sample output for the script: <pre>\$> ruby -v bad.rb ruby 2.6.3p62 (2019-04-16 revision 67580) [x86_64-darwin18] "jjjjjjjjjjjjjjjjjjjjjjjjjjjjjj" "D[D'\xFD\a\x00\xF0\x00\x00\x00\x00\x00\x00\x00\x90\x18\x00jjjjjj"</pre> This is caused by the same underlying issue as #15792. Credits to wanabe-san for using eval as a cross-version way of registering a fstring. I have a fix for this: https://github.com/ruby/ruby/pull/2183		

Associated revisions

Revision 9dec4e8fc3a6018261834b5ac9b9877f787b97ca - 06/18/2019 03:18 AM - alanwu (Alan Wu)

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
a = ('j' * 24).b.b
eval('', binding, a)

p a
4.times { GC.start }
p a
```

- string.c (str_replace_shared_without_enc): when given a dependent string, depend on the root of the dependent string.

[Bug #15934]

Revision 9dec4e8fc3a6018261834b5ac9b9877f787b97ca - 06/18/2019 03:18 AM - alanwu (Alan Wu)

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```

- string.c (str_replace_shared_without_enc): when given a dependent string, depend on the root of the dependent string.

[Bug #15934]

Revision 9dec4e8f - 06/18/2019 03:18 AM - alanwu (Alan Wu)

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```

- string.c (str_replace_shared_without_enc): when given a dependent string, depend on the root of the dependent string.

[Bug #15934]

Revision 8a94d4b0d4f988d4e6dc2d3556e2504f44afab4b - 08/07/2019 12:23 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca: [Backport #15934]

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
`ruby
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
`
```

- string.c (str_replace_shared_without_enc): when given a dependent string, depend on the root of the dependent string.

[Bug #15934]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67733 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 8a94d4b0d4f988d4e6dc2d3556e2504f44afab4b - 08/07/2019 12:23 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca: [Backport #15934]

```
String#b: Don't depend on dependent string
```

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
```ruby
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```
```

```
- string.c (str_replace_shared_without_enc): when given a
  dependent string, depend on the root of the dependent
  string.
```

[Bug #15934]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67733 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 8a94d4b0 - 08/07/2019 12:23 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca: [Backport #15934]

```
String#b: Don't depend on dependent string
```

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
```ruby
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```
```

```
- string.c (str_replace_shared_without_enc): when given a
  dependent string, depend on the root of the dependent
  string.
```

[Bug #15934]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67733 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision b49b1d76d116c4262819a86ca51cb6df19304b9f - 08/26/2019 04:09 PM - U.Nakamura

merge revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca: [Backport #15934]

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
```ruby
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```

...

- string.c (str\_replace\_shared\_without\_enc): when given a dependent string, depend on the root of the dependent string.

[Bug #15934]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby\_2\_5@67767 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

#### Revision b49b1d76d116c4262819a86ca51cb6df19304b9f - 08/26/2019 04:09 PM - U.Nakamura

merge revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca: [Backport #15934]

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
```ruby
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```
```

- string.c (str\_replace\_shared\_without\_enc): when given a dependent string, depend on the root of the dependent string.

[Bug #15934]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby\_2\_5@67767 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

#### Revision b49b1d76 - 08/26/2019 04:09 PM - U.Nakamura

merge revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca: [Backport #15934]

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to @wanabe for using eval as a cross-version way of registering a fstring.

```
```ruby
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```
```

- string.c (str\_replace\_shared\_without\_enc): when given a dependent string, depend on the root of the dependent string.

[Bug #15934]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby\_2\_5@67767 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

## History

### #1 - 06/18/2019 03:21 AM - alanwu (Alan Wu)

- Status changed from Open to Closed

Applied in changeset [git|9dec4e8fc3a6018261834b5ac9b9877f787b97ca](#).

---

String#b: Don't depend on dependent string

Registering a string that depend on a dependent string as fstring can lead to use-after-free. See c06ddfe and 3f95620 for details.

The following script triggers use-after-free on trunk, 2.4.6, 2.5.5 and 2.6.3. Credits to [@wanabe \(\\_wanabe\)](#) for using eval as a cross-version way of registering a fstring.

```
a = ('j' * 24).b.b
eval('', binding, a)
```

```
p a
4.times { GC.start }
p a
```

- string.c (str\_replace\_shared\_without\_enc): when given a dependent string, depend on the root of the dependent string.

[Bug [#15934](#)]

**#2 - 08/07/2019 10:59 AM - nagachika (Tomoyuki Chikanaga)**

- Backport changed from 2.4: UNKNOWN, 2.5: UNKNOWN, 2.6: UNKNOWN to 2.4: REQUIRED, 2.5: REQUIRED, 2.6: REQUIRED

**#3 - 08/07/2019 12:23 PM - nagachika (Tomoyuki Chikanaga)**

- Backport changed from 2.4: REQUIRED, 2.5: REQUIRED, 2.6: REQUIRED to 2.4: REQUIRED, 2.5: REQUIRED, 2.6: DONE

ruby\_2\_6 r67733 merged revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca.

**#4 - 08/26/2019 04:09 PM - usa (Usaku NAKAMURA)**

- Backport changed from 2.4: REQUIRED, 2.5: REQUIRED, 2.6: DONE to 2.4: REQUIRED, 2.5: DONE, 2.6: DONE

ruby\_2\_5 r67767 merged revision(s) 9dec4e8fc3a6018261834b5ac9b9877f787b97ca.