Ruby - Bug #15847

SecureRandom#gen_random becomes private after first invocation

05/13/2019 03:07 PM - graywolf (Gray Wolf)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.5.5p157 (2019-03-15 revision 67260) [x86_64-linux]	**Backport:**	2.4: DONTNEED, 2.5: DONE, 2.6: DONE

Description

There seems to be an issue with SecureRandom#gen_random becoming private after first invocation:

```
+   $ /tmp/my_ruby/bin/ruby -v
ruby 2.7.0dev (2019-05-13 trunk 082bbdc92e) [x86_64-linux]

$ /tmp/my_ruby/bin/ruby \
 -e 'require "securerandom"' \
 -e 'SecureRandom.gen_random(1)'

$ /tmp/my_ruby/bin/ruby \
 -e 'require "securerandom"' \
 -e 'SecureRandom.gen_random(1)' \
 -e 'SecureRandom.gen_random(1)'
Traceback (most recent call last):
-e:3:in `<main>': private method `gen_random' called for SecureRandom:Module (NoMethodError)
```

This is caused by using alias since 2.5 ruby in secure random class. Both .gen_random_openssl and .gen_random_urandom are private class method. Using the alias on them does not remove the private property, so new .gen_random is private as well. Patch fixing the issue:

```
diff --git a/lib/securerandom.rb b/lib/securerandom.rb
index 37835bf7df..2b0f3753b3 100644
--- a/lib/securerandom.rb
+++ b/lib/securerandom.rb
@@ -84,7 +84,8 @@ def gen_random(n)
           @rng_chooser.synchronize do
             class << self
               remove_method :gen_random
-              alias gen_random gen_random_openssl
+              alias_method(:gen_random, :gen_random_openssl)
+              public(:gen_random)
             end
           end
           return gen_random(n)
@@ -93,7 +94,8 @@ class << self
         @rng_chooser.synchronize do
           class << self
             remove_method :gen_random
-            alias gen_random gen_random_urandom
+            alias_method(:gen_random, :gen_random_urandom)
+            public(:gen_random)
           end
         end
         return gen_random(n)
```

This bug is not present in 2.4.6. First noticed on 2.5.5. Examples in this ticket are from current trunk.

Associated revisions

Revision 5bab1304af25a843728dbcd2f3594913740aecb0 - 05/14/2019 02:44 AM - shyouhei (Shyouhei Urabe)

fix visibility of SecureRandom.gen_random

Aliasing a method preserves its visibility. These aliases turn
formerly-public methods into private. Should make them public
again. [Bug #15847]

Revision 5bab1304af25a843728dbcd2f3594913740aecb0 - 05/14/2019 02:44 AM - shyouhei (Shyouhei Urabe)

fix visibility of SecureRandom.gen_random

Aliasing a method preserves its visibility. These aliases turn
formerly-public methods into private. Should make them public
again. [Bug #15847]

Revision 5bab1304 - 05/14/2019 02:44 AM - shyouhei (Shyouhei Urabe)

fix visibility of SecureRandom.gen_random

Aliasing a method preserves its visibility. These aliases turn
formerly-public methods into private. Should make them public
again. [Bug #15847]

Revision a451d5d303459e26f5d55f6a5a8a08492f98e849 - 08/01/2019 01:18 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0: [Backport #15847]

```
    fix visibility of SecureRandom.gen_random

    Aliasing a method preserves its visibility.  These aliases turn
    formerly-public methods into private.  Should make them public
    again.  [Bug #15847]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67723 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a451d5d303459e26f5d55f6a5a8a08492f98e849 - 08/01/2019 01:18 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0: [Backport #15847]

```
    fix visibility of SecureRandom.gen_random

    Aliasing a method preserves its visibility.  These aliases turn
    formerly-public methods into private.  Should make them public
    again.  [Bug #15847]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67723 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision a451d5d3 - 08/01/2019 01:18 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0: [Backport #15847]

```
    fix visibility of SecureRandom.gen_random

    Aliasing a method preserves its visibility.  These aliases turn
    formerly-public methods into private.  Should make them public
    again.  [Bug #15847]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_6@67723 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7cdacb99ad17c859dc701843bd37d49412305716 - 08/26/2019 03:13 PM - U.Nakamura

merge revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0: [Backport #15847]

```
    fix visibility of SecureRandom.gen_random

    Aliasing a method preserves its visibility.  These aliases turn
    formerly-public methods into private.  Should make them public
    again.  [Bug #15847]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@67762 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7cdacb99ad17c859dc701843bd37d49412305716 - 08/26/2019 03:13 PM - U.Nakamura

merge revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0: [Backport #15847]

```
    fix visibility of SecureRandom.gen_random

    Aliasing a method preserves its visibility.  These aliases turn
    formerly-public methods into private.  Should make them public
    again.  [Bug #15847]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@67762 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 7cdacb99 - 08/26/2019 03:13 PM - U.Nakamura

merge revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0: [Backport #15847]

```
    fix visibility of SecureRandom.gen_random

    Aliasing a method preserves its visibility.  These aliases turn
    formerly-public methods into private.  Should make them public
    again.  [Bug #15847]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_5@67762 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 05/14/2019 02:47 AM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Closed

Applied in changeset git|5bab1304af25a843728dbcd2f3594913740aecb0.

---

fix visibility of SecureRandom.gen_random

Aliasing a method preserves its visibility. These aliases turn
formerly-public methods into private. Should make them public
again. [Bug #15847]

#2 - 05/14/2019 02:50 AM - shyouhei (Shyouhei Urabe)

Thank you for reporting! It was my fault. have just pushed a fix.

#3 - 05/14/2019 05:43 AM - nagachika (Tomoyuki Chikanaga)

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

#4 - 08/01/2019 01:18 PM - nagachika (Tomoyuki Chikanaga)

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

ruby_2_6 r67723 merged revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0.

#5 - 08/26/2019 03:13 PM - usa (Usaku NAKAMURA)

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

ruby_2_5 r67762 merged revision(s) 5bab1304af25a843728dbcd2f3594913740aecb0.