

Ruby - Bug #19230

The openssl backend of securerandom is no longer needed

12/13/2022 07:37 AM - mame (Yusuke Endoh)

Status:	Closed	
Priority:	Normal	
Assignee:	shyouhei (Shyouhei Urabe)	
Target version:		
ruby -v:	ruby 3.1.3p185 (2022-11-24 revision 1a6b16756e) [x86_64-linux]	Backport: 2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN

Description

securerandom first checks if Random.urandom is available ([Line 77](#)), and if not available, it uses the openssl backend as a degeneration. However, the openssl backend does not work because it internally uses Random.urandom ([Line 55](#)) to create a seed. This issue is found by @hanachin.

```
$ ruby -ve 'def Random.urandom(*); raise; end; require "securerandom"; p SecureRandom.bytes(10) '
ruby 3.1.3p185 (2022-11-24 revision 1a6b16756e) [x86_64-linux]
-e:1: warning: method redefined; discarding old urandom
-e:1:in `urandom': unhandled exception
      from /home/mame/local/lib/ruby/3.1.0/securerandom.rb:75:in `singleton class'
      from /home/mame/local/lib/ruby/3.1.0/securerandom.rb:42:in `'
      from /home/mame/local/lib/ruby/3.1.0/securerandom.rb:41:in `'
      from <internal:/home/mame/local/lib/ruby/3.1.0/rubygems/core_ext/kernel_require.rb>:85:in
`require'
      from <internal:/home/mame/local/lib/ruby/3.1.0/rubygems/core_ext/kernel_require.rb>:85:in
`require'
      from -e:1:in `'
```

There has been this bug since [abae70d6ed63054d7d01bd6cd80c1b5b98b93ba3](#), which made the urandom backend as default and left the openssl backend just for degeneration. I think no one need the openssl anymore because no one has reported this bug for such a long time.

How about removing it?

```
diff --git a/lib/securerandom.rb b/lib/securerandom.rb
index 07ae048634..32b76a2137 100644
--- a/lib/securerandom.rb
+++ b/lib/securerandom.rb
@@ -14,7 +14,6 @@
#
# It supports the following secure random number generators:
#
-# * openssl
# * /dev/urandom
# * Win32
#
@@ -46,21 +45,6 @@ def bytes(n)

  private

  def gen_random_openssl(n)
    @pid = 0 unless defined?(@pid)
    pid = $$
    unless @pid == pid
      now = Process.clock_gettime(Process::CLOCK_REALTIME, :nanosecond)
      OpenSSL::Random.random_add([now, @pid, pid].join(""), 0.0)
      seed = Random.urandom(16)
      if (seed)
        OpenSSL::Random.random_add(seed, 16)
      end
      @pid = pid
    end
  end
end
```

```

-     end
-     return OpenSSL::Random.random_bytes(n)
- end
-
-   def gen_random_urandom(n)
-     ret = Random.urandom(n)
-     unless ret
@@ -77,13 +61,7 @@ def gen_random_urandom(n)
-     Random.urandom(1)
-     alias gen_random gen_random_urandom
- rescue RuntimeError
-   begin
-     require 'openssl'
-     rescue NoMethodError
-       raise NotImplementedError, "No random device"
-     else
-       alias gen_random gen_random_openssl
-     end
+     raise NotImplementedError, "No random device"
-   end
-
-   public :gen_random

```

History

#1 - 12/13/2022 08:56 AM - zzak (zzak _)

Good catch!

I did a quick GitHub search to see if anyone might be calling this method directly, but given it's private maybe we shouldn't care? The first 10 pages showed no interesting results.

It seems [this test](#) will have to be removed, also in the gem, which seems like mame-san added :)

There was also [this ticket](#) in JRuby, which I guess means they Charlie can remove that exclusion from their test suite..

#2 - 02/26/2023 11:17 AM - dentarg (Patrik Ragnarsson)

Here's actually an user running into the above bug: <https://github.com/stefansundin/rssbox/issues/67>, <https://github.com/sinatra/sinatra/pull/1888>

but removing this code would address the issue too as Sinatra has some sort of fallback implemented

#3 - 03/09/2023 05:08 AM - mame (Yusuke Endoh)

- Status changed from Open to Assigned

- Assignee set to shyuhei (Shyouhei Urabe)

#4 - 04/13/2023 07:01 AM - shyuhei (Shyouhei Urabe)

Proposed fix: <https://github.com/ruby/ruby/pull/7705>

#5 - 08/31/2023 03:39 AM - jeremyevans0 (Jeremy Evans)

- Status changed from Assigned to Closed

Fixed by [64e503eb62aff0952b655e9a86217e355f786146](https://github.com/ruby/ruby/commit/64e503eb62aff0952b655e9a86217e355f786146)