

We Interrupt Your Regularly Scheduled Programming to Bring You
A Public Service Announcement

Use *rand* module now¹

¹ Unless you stick to the older Erlang/OTP or Elixir versions before Erlang/OTP 18.x

**The random module is
obsolete**

and will be compromised by a brute-force attack in 9 hours!²

² <https://github.com/jj1bdx/as183-c>

Still many examples use
random:uniform/1
This is not good

Stop using *random* module now³

³ Unless you stick to the older Erlang/OTP or Elixir versions before Erlang/OTP 18.x

Use `rand:uniform/1`
or `:rand.uniform()`

Alternatives

- exsplus116, equivalent to rand module's default algorithm, for 17.x or older versions of Erlang/OTP
 - sfmt-erlang (hex.pm: sfmt)
 - tinymt-erlang (hex.pm: tinymt)

I repeat:
use *rand* module
right now⁴!

⁴ Unless you stick to the older Erlang/OTP or Elixir versions before Erlang/OTP 18.x

**random module will be
deprecated in OTP 19
removed from OTP 20**

(Officially announced by Kenneth Lundin on Erlang
Factory SF Bay 2016 Day 1)

Thank you