Ruby - Bug #5110

Ruby SSL error - sslv3 alert unexpected message

07/28/2011 08:56 AM - hoisie (Michael Hoisie)

Status:	Closed		
Priority:	Normal		
Assignee:	MartinBosslet (Martin Bosslet)		
Target version:	1.9.3		
ruby -v:	ruby 1.9.2p290	**Backport:**	

Description

I'm running ruby 1.9.2p290 on a machine with OpenSSL version 0.9.8o 01 Jun 2010

When I run the following script:

```
require 'net/http'
url = URI.parse('https://www.xpiron.com/schedule')
req = Net::HTTP::Get.new(url.path)
sock = Net::HTTP.new(url.host, 443)
sock.use_ssl = true
sock.start do |http|
response = http.request(req)
end
```

It generates an error:

/usr/local/lib/ruby/1.9.1/net/http.rb:678:in connect': SSL_connect returned=1 errno=0 state=SSLv2/v3 read server hello A: sslv3 alert unexpected message (OpenSSL::SSL::SSLError) from /usr/local/lib/ruby/1.9.1/net/http.rb:678:in block in connect'
from /usr/local/lib/ruby/1.9.1/timeout.rb:44:in timeout' from /usr/local/lib/ruby/1.9.1/timeout.rb:89:in timeout'
from /usr/local/lib/ruby/1.9.1/net/http.rb:678:in connect' from /usr/local/lib/ruby/1.9.1/net/http.rb:637:in do_start'
from /usr/local/lib/ruby/1.9.1/net/http.rb:626:in start' from test.rb:8:in '

If I add the following line, it works:
sock.ssl_version="SSLv3"

The HTTPS server seems to be misconfigured, but it may also be an issue with how Ruby's HTTP library negotiates SSL connections.

History

#1 - 08/01/2011 12:54 AM - MartinBosslet (Martin Bosslet)

- Category set to ext

- Status changed from Open to Feedback

- Assignee set to MartinBosslet (Martin Bosslet)

- Target version set to 1.9.3

In my opinion Ruby reacts normal here. The OpenSSL::SSL::SSLContext is allocated using "SSLv23" by default for maximum compatibility. Here is what the official doc says:

SSLv23_method:

A TLS/SSL connection established with these methods will understand the SSLv2, SSLv3, and TLSv1 protocol. A client will send out SSLv2 client hello messages and will indicate that it also understands SSLv3 and TLSv1. A server will understand SSLv2, SSLv3, and TLSv1 client hello messages. This is the best choice when compatibility is a concern.

I checked, the server you mentions does accept v3 client hello messages only, so it does not recognize in particular the v2 message that is sent by default. I'd suggest that it is fine to blame the server for being inflexible in your case.

Do you agree?

Regards,
Martin

#2 - 10/19/2011 11:14 AM - MartinBosslet (Martin Bosslet)

- Status changed from Feedback to Closed

If nobody disagrees, I would like to close this.