Ruby - Bug #12309

Segmentation fault caused by OpenSSL

04/22/2016 09:18 AM - jhaig (Joseph Haig)

Status:	Rejected		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.3.0p0 (2015-12-25 revision 53290) [x86_64-linux]	**Backport:**	2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN

Description

I am consistently getting a segmentation fault whils running Sinatra. It appears to be during an net/http request to an ssl endpoint on a remote web server. The full stack trace is below.

Sinatra runs correctly for a few minutes, making numerous requests with net/http, but then fails with the segmentation fault. I can find nothing particularly unusual with either the offending request or its response.

I am using an up-to-date version of Ubuntu 14.04 LTS.

```
$ ruby -ropenssl -e 'p OpenSSL::OPENSSL_VERSION'
"OpenSSL 1.0.1f 6 Jan 2014"
```

Related issues:

Related to Ruby - Bug #12292: Race between OpenSSL::SSL::SSLSocket#stop and #...	**Closed**

History

#1 - 04/22/2016 01:58 PM - nobu (Nobuyoshi Nakada)

- File bug-12309.log added

- Description updated

Maybe [Bug #12126]?

#2 - 06/07/2016 07:18 AM - naruse (Yui NARUSE)

- Related to Bug #12126: [PATCH] openssl: accept moving write buffer for write_nonblock added

#3 - 06/07/2016 07:19 AM - naruse (Yui NARUSE)

- Related to Bug #6168: Segfault in OpenSSL bindings added

#4 - 10/23/2016 03:19 PM - rhenium (Kazuki Yamaguchi)

- Related to deleted (Bug #6168: Segfault in OpenSSL bindings)

#5 - 10/23/2016 03:23 PM - rhenium (Kazuki Yamaguchi)

- Status changed from Open to Rejected

It looks like the same issue as [Bug #12292] rather than [Bug #12126], because #12126 should not be a cause of a segfault. (and net/http does not use SSLSocket#write_nonblock, does it?)

Please provide a reproducer if it is a different issue.

#6 - 10/23/2016 03:23 PM - rhenium (Kazuki Yamaguchi)

- Related to deleted (Bug #12126: [PATCH] openssl: accept moving write buffer for write_nonblock)

#7 - 10/23/2016 03:23 PM - rhenium (Kazuki Yamaguchi)

- Related to Bug #12292: Race between OpenSSL::SSL::SSLSocket#stop and #connect can cause a segmentation fault added

Files

bug-12309.log		82.6 KB	04/22/2016	nobu (Nobuyoshi Nakada)