Ruby master - Bug #9592
Fix segfault with old OpenSSL
03/05/2014 03:13 AM - nobu (Nobuyoshi Nakada)

Status: Closed
Priority: Normal
Assignee: 
Target version: 2.2.0
ruby -v: r45270
Backport: 1.9.3: DONE, 2.0.0: DONE, 2.1: DONE

Description
r44572 旧なOpenSSL(0.9.8kご近所)でSSL connectionに失敗したときにSEGVが発生します。
$ ruby -rnet/https -e 'Net::HTTP.get(URI("https://brandymelvilleusa.com"))'
/app/vendor/ruby-2.0.0/lib/ruby/2.0.0/net/http.rb:918: [BUG] Segmentation fault
ruby 2.0.0p451 (2014-02-24 revision 45167) [x86_64-linux]
r45271 修正をしたのでバックポートをお願いします。

Related issues:
Related to Backport193 - Backport #9672: backport r45271 Closed 03/25/2014
Has duplicate Ruby master - Bug #9839: Segment fault in http Rejected

Revision 0cc54369 - 03/30/2014 02:50 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45271: [Backport #9592] [Backport #9670]

* ext/openssl/ossl.c (ossl_make_error): check NULL for unknown error reasons with old OpenSSL, and insert a colon iff formatted message is not empty.

Revision 45472 - 03/30/2014 02:50 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45271: [Backport #9592] [Backport #9670]

* ext/openssl/ossl.c (ossl_make_error): check NULL for unknown error reasons with old OpenSSL, and insert a colon iff formatted message is not empty.

Revision 49fed341 - 05/01/2014 03:23 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45271: [Backport #9592] [Backport #9671]

* ext/openssl/ossl.c (ossl_make_error): check NULL for unknown error reasons with old OpenSSL, and insert a colon iff formatted message is not empty.

Revision 45778 - 05/01/2014 03:23 PM - nagachika (Tomoyuki Chikanaga)
merge revision(s) r45271: [Backport #9592] [Backport #9671]

* ext/openssl/ossl.c (ossl_make_error): check NULL for unknown error reasons with old OpenSSL, and insert a colon iff formatted message is not empty.

History
#1 - 03/05/2014 03:14 AM - nobu (Nobuyoshi Nakada)
- Description updated

#2 - 03/11/2014 11:46 PM - nobu (Nobuyoshi Nakada)
security fixではないですが、明らかなregressionなので1.9.3にも必要かもしれません。

#3 - 03/30/2014 02:50 PM - nagachika (Tomoyuki Chikanaga)
- Status changed from Open to Closed
- % Done changed from 0 to 100

Applied in changeset ruby-200:r45472.

merge revision(s) r45271: [Backport #9592] [Backport #9670]

* ext/openssl/ossl.c (ossl_make_error): check NULL for unknown error reasons with old OpenSSL, and insert a colon iff formatted message is not empty.

#4 - 03/30/2014 02:53 PM - nagachika (Tomoyuki Chikanaga)
- Backport changed from 1.9.3: REQUIRED, 2.0.0: REQUIRED, 2.1: REQUIRED to 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: REQUIRED

r45271 was backported to ruby_2_0_0 at r45472.

コミット連動で閉じてしまいましたが、trunk では修正済みなので Closed にした上で Backport 欄を使うということでそのままにしておきます。

#5 - 03/31/2014 06:38 AM - usa (Usaku NAKAMURA)
- Related to Backport #9672: backport r45271 added

#6 - 03/31/2014 06:39 AM - usa (Usaku NAKAMURA)
- Backport changed from 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: REQUIRED to 1.9.3: DONE, 2.0.0: DONE, 2.1: REQUIRED

backported into ruby_1_9_3 at r45485. (see #9672)

#7 - 04/28/2014 07:53 PM - nathany (Nathan Youngman)
We saw this error in production with Ruby 2.1.1p76 on Heroku, but I don't know how to reproduce it. Is a backport to 2.1.1 planned? Or including the fix in 2.1.2?

Apr 22 08:03:01 app/worker.1: /app/vendor/ruby-2.1.1/lib/ruby/2.1.0/net/http.rb:920: [BUG] Segmentation fault at 0x00000000000000
Apr 22 08:03:01 app/worker.1: ruby 2.1.1p76 (2014-02-24 revision 45161) [x86_64-linux]

#8 - 04/29/2014 02:25 AM - nobu (Nobuyoshi Nakada)
I suspect it occurs only with very old version OpenSSL, I can't reproduce it on other platforms at least.

It is planned to backport to 2.1, and the next 2.1 will be 2.1.2.

#9 - 04/29/2014 09:26 PM - nathany (Nathan Youngman)

Nobuyoshi Nakada wrote:

I suspect it occurs only with very old version OpenSSL, I can't reproduce it on other platforms at least.

Yes, Heroku is running OpenSSL 0.9.8k 25 Mar 2009 on their Cedar stack.
(heroku run openssl version)

It is planned to backport to 2.1, and the next 2.1 will be 2.1.2.

Thanks. Looking forward to 2.1.2.

#10 - 05/01/2014 03:24 PM - nagachika (Tomoyuki Chikanaga)
- Backport changed from 1.9.3: DONE, 2.0.0: DONE, 2.1: REQUIRED to 1.9.3: DONE, 2.0.0: DONE, 2.1: DONE

r45271 was backported into ruby_2_1 branch at r45778.

#11 - 10/24/2016 07:27 AM - rhenium (Kazuki Yamaguchi)
- Has duplicate Bug #9839: Segment fault in http added