

Ruby trunk - Bug #4445

ext/openssl verify_callback rb_protect

02/25/2011 12:09 AM - ohai (Ippei Obayashi)

Status: Closed	
Priority: Normal	
Assignee: nahi (Hiroshi Nakamura)	
Target version: 1.9.3	
ruby -v: ruby 1.9.2p180 (2011-02-18 revision 30909) [x86_64-linux]	Backport:
Description =begin openssl callback rb_protect openssl SEGV =end	

Associated revisions

Revision ab86f1cf - 07/14/2011 05:41 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi. See #4445.
- test/openssl/test_ssl.rb (test_exception_in_verify_callback_is_ignored): test it.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32537 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32537 - 07/14/2011 05:41 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi. See #4445.
- test/openssl/test_ssl.rb (test_exception_in_verify_callback_is_ignored): test it.

Revision 32537 - 07/14/2011 05:41 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback

causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi.
See #4445.

- test/openssl/test_ssl.rb
(test_exception_in_verify_callback_is_ignored): test it.

Revision 32537 - 07/14/2011 05:41 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi. See #4445.
- test/openssl/test_ssl.rb
(test_exception_in_verify_callback_is_ignored): test it.

Revision 32537 - 07/14/2011 05:41 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi. See #4445.
- test/openssl/test_ssl.rb
(test_exception_in_verify_callback_is_ignored): test it.

Revision 32537 - 07/14/2011 05:41 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi. See #4445.
- test/openssl/test_ssl.rb
(test_exception_in_verify_callback_is_ignored): test it.

Revision 32537 - 07/14/2011 05:41 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi. See #4445.
- test/openssl/test_ssl.rb
(test_exception_in_verify_callback_is_ignored): test it.

Revision bdd7cf15 - 07/14/2011 05:46 AM - nahi (Hiroshi Nakamura)

- backport r32537 from trunk.
- ext/openssl/openssl.c (ossl_verify_cb): trap the exception from verify callback of SSLContext and X509Store and make the verification fail normally. Raising exception directly from callback causes orphan resources in OpenSSL stack. Patched by Ippei Obayashi. See #4445.
- test/openssl/test_ssl.rb (test_exception_in_verify_callback_is_ignored): test it.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@32538 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 06/26/2011 06:12 PM - naruse (Yui NARUSE)

- Status changed from Open to Assigned
- Assignee set to nahi (Hiroshi Nakamura)

#2 - 06/26/2011 06:44 PM - nahi (Hiroshi Nakamura)

- Target version set to 1.9.3

#3 - 06/26/2011 11:57 PM - nahi (Hiroshi Nakamura)

- Assignee changed from nahi (Hiroshi Nakamura) to MartinBosslet (Martin Bosslet)

Martin, can you handle this? Original reporter said that verify_cb does not use rb_protect to invoke a callback so an error raised from the callback passed directly to Ruby interpreter. Proposed patch looks good but we should check the rational of the current code (svn blame & svn log) and do some test around this.

#4 - 06/27/2011 08:23 PM - MartinBosslet (Martin Bosslet)

Yes, I'll look into it!

#5 - 06/28/2011 10:26 PM - nahi (Hiroshi Nakamura)

Note: [#4611](#) and [#4875](#) both crashes at ossl_ssl_verify_callback (1.9.2p274, 1.9.2p180.) I suspected this issue related to those issues.

#6 - 06/28/2011 11:46 PM - MartinBosslet (Martin Bosslet)

Thanks for the input, I will keep them in mind when investigating this!

#7 - 07/12/2011 06:24 PM - nahi (Hiroshi Nakamura)

Martin, how's the status? Can I take over this issue again? I think [#4875](#) and [#4611](#) relates to this issue.

#8 - 07/12/2011 11:34 PM - MartinBosslet (Martin Bosslet)

- Assignee changed from MartinBosslet (Martin Bosslet) to nahi (Hiroshi Nakamura)

Hiroshi Nakamura wrote:

Martin, how's the status? Can I take over this issue again? I think [#4875](#) and [#4611](#) relates to this issue.

Sure - if you feel it's related to the other two issues then you are clearly in a better position to design this properly. Should I look into [#4923](#) and [#4961](#) instead? Or are there any other urgencies where I could help?

#9 - 07/13/2011 02:43 PM - nahi (Hiroshi Nakamura)

[#4611#4875](#)

Obayashi Obayashi callback verify callback OpenSSL

1.9.4 verify_callback → SSL SSLerror X509Store

1.9.3 rb_jump_tag deprecation verify_callback

#10 - 07/13/2011 04:28 PM - nahi (Hiroshi Nakamura)

Martin Bosslet wrote:

Sure - if you feel it's related to the other two issues then you are clearly in a better position to design this properly. Should I look into [#4923](#) and [#4961](#) instead? Or are there any other urgencies where I could help?

OK, I take this.

Do you think you can handle [#4961](#)? I don't think it's a release blocker since we just added tests which does not run with OpenSSL 0.9.7. It has not yet worked ever. But there could be a chance to find a easy way to fix the bug.

#11 - 07/13/2011 07:18 PM - MartinBosslet (Martin Bosslet)

Hiroshi Nakamura wrote:

Do you think you can handle [#4961](#)? I don't think it's a release blocker since we just added tests which does not run with OpenSSL 0.9.7. It has not yet worked ever. But there could be a chance to find a easy way to fix the bug.

I tried OpenSSL.decode on the PEM data and it was valid. I'll try my best, probably debugging it directly in C will show us what fails there.

So I will concentrate on [#4961](#), and if I can solve that, I will continue on [#4923](#). If I can help you with anything, please let me know!

#12 - 07/14/2011 02:52 PM - nahi (Hiroshi Nakamura)

- Status changed from Assigned to Closed

```
r32537 trunk r32538 ruby_1_9_3 Obayashi patch warn
SSLError GC
```

```
: verify callback warn SSLError
```

```
Obayashi
```

Files

verify_cb.diff	662 Bytes	02/25/2011	ohai (Ippei Obayashi)
----------------	-----------	------------	-----------------------