Ruby master - Bug #4445

ext/openssl の verify_callback が rb_protect で保護されていない

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 では 証明書の検証に付加的な機能を付けるための
callback を設定できます。これをrubyから利用できるようになっていますが
rb_protect を使っていないため、openssl ライブラリ内部を飛び越えて
例外が飛ぶようになってしまう状態です。

現在ではSEGVが発生する等の問題は見つかってはいませんがメモリリークなど
起きている可能性が高いです。

とりあえず大域脱出を止めるパッチを添付します。例外を適当な場所で再送するべきかもしれませんが
それはしていません。
=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 resouces 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 resouces 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 resouces 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 resouces 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 resouces 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 resouces 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 resouces 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/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 resouces 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)

騒いでおいてすいません。 #4611#4875 へのリンクを外しました。ちゃんとスタックを見たら、関係ありませんでした。

で、このチケットですが、Obayashiのおっしゃる通り、確かに今のコードはダメですね。他のcallback同様、事後に例外を上げられるといいんですが、verify callbackはOpenSSL側から何度も呼ばれるので、「事後」がうまく定義できません。

というわけで、1.9.4ではverify_callback内での例外は検証失敗扱いにしようと思います。（従来のようには例外は上がらない→SSLの場合は別途SSLErrorが上がる。X509Storeの場合はただの検証失敗になる）

ただ、1.9.3でどうするか悩んでいます。↑の変更を入れてしまいたいところですが、どこかで例外を投げているカスタマイズされたverify_callbackを見たことがあります。この時期に非互換を入れるのも。。。というわけで、挙動は従来どおりとして、rb_jump_tagの前にdeprecation警告、とかかなあ。。。

#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でtrunk ´r32538でruby_1_9_3を修正しました。結果的には、Obayashiさん（前回呼び捨てですいません）のpatchをそのまま当て、かつ例外を投げている場合にはwarnで警告をする（しかし無視して、通常の検証失敗とする）ようにしました。テストを書いてみたらSSL接続が残ったままになり、GCで回収されるまでそのままという、いかにも危ない挙動になった（当たり前）ので、この時期ではありますが対処しました。

挙動変更は以下です: verify callbackで例外を投げた場合、従来はその例外が飛んでいましたが、代わりにwarnでやめろと警告され、SSLErrorが上がるようになります。

Obayashiさん、ご報告ありがとうございました。

Files

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