[PATCH] OpenSSL::SSL::SSLcontext#{alpn,npn}_select_cb= does not work properly

12/12/2015 05:34 PM - rhenium (Kazuki Yamaguchi)

Status: Closed
Priority: Normal
Assignee: 
Target version:
ruby -v: ruby 2.3.0dev (2015-12-13 trunk 53061) [x86_64-linux]
Backport: 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: DONE

Description
The protocol list passed to the callback function (set by SSL_CTX_set_alpn_select_cb, SSL_CTX_set_next_proto_select_cb) is not null-terminated string.

This issue seems to have been existing since first NPN was supported (r36871).

This patch also removes the code checking the length of protocol name, because it is already validated by OpenSSL.

Associated revisions
Revision 30238f96 - 11/15/2016 06:33 AM - usa (Usaku NAKAMURA)
merge revision(s) 53064: [Backport #11810]

* extopenssl/ossl_ssl.c (ssl_npn_select_cb_common): fix parsing protocol list. The protocol list from OpenSSL is not null-terminated. patched by Kazuki Yamaguchi [Bug #11810] [ruby-core:72082]
git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@56798 b2dd03c8-39d4-4d8f-98ff-823fe69b080e
* ext/openssl/ossl_ssl.c (ssl_npn_select_cb_common): fix parsing protocol list. The protocol list from OpenSSL is not null-terminated. patched by Kazuki Yamaguchi [Bug #11810] [ruby-core:72082]

History

#1 - 12/13/2015 01:30 AM - naruse (Yui NARUSE)
- Status changed from Open to Closed

Applied in changeset r53064.

- ext/openssl/ossl_ssl.c (ssl_npn_select_cb_common): fix parsing protocol list. The protocol list from OpenSSL is not null-terminated. patched by Kazuki Yamaguchi [Bug #11810] [ruby-core:72082]

#2 - 11/15/2016 06:33 AM - usa (Usaku NAKAMURA)
- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: DONE

ruby_2_2 r56798 merged revision(s) 53064.

Files

0001-ext-openssl-ossl_ssl.c-ssl_npn_select_cb_common-fix-.patch 1.27 KB 12/12/2015 rhenium (Kazuki Yamaguchi)