Ruby trunk - Bug #9644

ssl hostname verification security bug: verify_certificate_identity wildcard matching allows to much

03/16/2014 10:46 PM - noxxi (Steffen Ullrich)

Status:	Closed		
Priority:	Normal		
Assignee:	MartinBosslet (Martin Bosslet)		
Target version:	2.2.0		
ruby -v:	1.9, 2.0, 2.1	**Backport:**	1.9.3: REQUIRED, 2.0.0: DONE, 2.1: DONE

Description

Hi,
I'm not a ruby developer but the maintainer of the IO::Socket::SSL module in Perl. While comparing the state of the SSL implementations in various languages I've noticed, that your validation of the hostname inside the certificate is wrong regarding wildcards.

According to the RFC2818 (http) or RFC6125 (includes http and others) only the leftmost part of the name specification might contain a wildcard, e.g *.foo.bar is allowed, but not www.*.foo.bar or even www.*.*.*. Unfortunatly the implementation of verify_certificate_identity in openssl/ssl.rb (or openssl/ssl-internal.rb in older versions) does a global substitution of * with [^.]+ and thus allows wildcards anywhere and also multiple wildcards. I've verified my assumption with a certificate for www.*.foo.*, which got successfully verified against www.bar.foo.org or www.foobar.foo.bar on ruby 1.9.1. And, from looking at the code the current ruby version has the same problem.

Also, from reading the code I understand that you use the same hostname verification for SMTP, IMAP and POP too. But the verification schemes for these protocols differ from http (see RFC2595 for SMTP, RFC4642 for IMAP and POP):

- while http allows something like www*.example.com the other protocols only allow *.example.com, e.g. the the wildcard must fully replace the leftmost part of the hostname.
- while with http one should not check the common name if subject alternative names exist (and you've implemented it this way), with the other protocols one check common name too.

Regards,
Steffen

Associated revisions

Revision 599bfa72 - 04/13/2015 01:09 PM - nagachika (Tomoyuki Chikanaga)

- ext/openssl/lib/openssl/ssl.rb: stricter hostname verification following RFC 6125. with the patch provided by Tony Arcieri and Hiroshi Nakamura [ruby-core:61545] [Bug #9644]
- test/openssl/test_ssl.rb: add tests for above.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@50292 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 50292 - 04/13/2015 01:09 PM - nagachika (Tomoyuki Chikanaga)

- ext/openssl/lib/openssl/ssl.rb: stricter hostname verification following RFC 6125. with the patch provided by Tony Arcieri and Hiroshi Nakamura [ruby-core:61545] [Bug #9644]
- test/openssl/test_ssl.rb: add tests for above.

Revision 50292 - 04/13/2015 01:09 PM - nagachika (Tomoyuki Chikanaga)

- ext/openssl/lib/openssl/ssl.rb: stricter hostname verification following RFC 6125. with the patch provided by Tony Arcieri and Hiroshi Nakamura [ruby-core:61545] [Bug #9644]
- test/openssl/test_ssl.rb: add tests for above.

Revision 50292 - 04/13/2015 01:09 PM - nagachika (Tomoyuki Chikanaga)

- ext/openssl/lib/openssl/ssl.rb: stricter hostname verification following RFC 6125. with the patch provided by Tony Arcieri and Hiroshi Nakamura [ruby-core:61545] [Bug #9644]
- test/openssl/test_ssl.rb: add tests for above.

Revision 50292 - 04/13/2015 01:09 PM - nagachika (Tomoyuki Chikanaga)

- ext/openssl/lib/openssl/ssl.rb: stricter hostname verification following RFC 6125. with the patch provided by Tony Arcieri and Hiroshi Nakamura [ruby-core:61545] [Bug #9644]
- test/openssl/test_ssl.rb: add tests for above.

Revision 50292 - 04/13/2015 01:09 PM - nagachika (Tomoyuki Chikanaga)

- ext/openssl/lib/openssl/ssl.rb: stricter hostname verification following RFC 6125. with the patch provided by Tony Arcieri and Hiroshi Nakamura [ruby-core:61545] [Bug #9644]
- test/openssl/test_ssl.rb: add tests for above.

Revision 15edfd96 - 04/13/2015 01:13 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 50292: [Backport #9644]

```
* ext/openssl/lib/openssl/ssl.rb: stricter hostname verification
  following RFC 6125. with the patch provided by Tony Arcieri and
  Hiroshi Nakamura [ruby-core:61545] [Bug #9644]

* test/openssl/test_ssl.rb: add tests for above.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@50293 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 50293 - 04/13/2015 01:13 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 50292: [Backport #9644]

```
* ext/openssl/lib/openssl/ssl.rb: stricter hostname verification
  following RFC 6125. with the patch provided by Tony Arcieri and
  Hiroshi Nakamura [ruby-core:61545] [Bug #9644]

* test/openssl/test_ssl.rb: add tests for above.
```

Revision 329ab042 - 04/13/2015 01:16 PM - usa (Usaku NAKAMURA)

merge revision(s) 50292: [Backport #9644]

```
* ext/openssl/lib/openssl/ssl.rb: stricter hostname verification
  following RFC 6125. with the patch provided by Tony Arcieri and
  Hiroshi Nakamura [ruby-core:61545] [Bug #9644]

* test/openssl/test_ssl.rb: add tests for above.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_0_0@50294 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 50294 - 04/13/2015 01:16 PM - usa (Usaku NAKAMURA)

merge revision(s) 50292: [Backport #9644]

```
* ext/openssl/lib/openssl/ssl.rb: stricter hostname verification
  following RFC 6125. with the patch provided by Tony Arcieri and
  Hiroshi Nakamura [ruby-core:61545] [Bug #9644]

* test/openssl/test_ssl.rb: add tests for above.
```

Revision e3252606 - 04/13/2015 01:20 PM - usa (Usaku NAKAMURA)

merge revision(s) 50292: [Backport #9644]

```
* ext/openssl/lib/openssl/ssl.rb: stricter hostname verification
  following RFC 6125. with the patch provided by Tony Arcieri and
  Hiroshi Nakamura [ruby-core:61545] [Bug #9644]

* test/openssl/test_ssl.rb: add tests for above.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@50296 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 50296 - 04/13/2015 01:20 PM - usa (Usaku NAKAMURA)

merge revision(s) 50292: [Backport #9644]

```
* ext/openssl/lib/openssl/ssl.rb: stricter hostname verification
  following RFC 6125. with the patch provided by Tony Arcieri and
```

```
  Hiroshi Nakamura [ruby-core:61545] [Bug #9644]

* test/openssl/test_ssl.rb: add tests for above.
```

History

#1 - 03/17/2014 01:36 AM - nobu (Nobuyoshi Nakada)

- Description updated

- Category set to ext/openssl

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

- Priority changed from Normal to 5

- Target version set to 2.2.0

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN to 1.9.3: REQUIRED, 2.0.0: REQUIRED, 2.1: REQUIRED

Seems no wildcard tests.

#2 - 04/11/2015 05:53 AM - hansdegraaff (Hans de Graaff)

It looks like this is fixed with https://github.com/ruby/openssl/commit/e9a7bcb8bf2902f907c148a00bbcf21d3fa79596 which is related to https://bugzilla.redhat.com/show_bug.cgi?id=1209981

#3 - 04/13/2015 01:09 PM - nagachika (Tomoyuki Chikanaga)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

Applied in changeset r50292.

- ext/openssl/lib/openssl/ssl.rb: stricter hostname verification following RFC 6125. with the patch provided by Tony Arcieri and Hiroshi Nakamura [ruby-core:61545] [Bug #9644]
- test/openssl/test_ssl.rb: add tests for above.

#4 - 04/13/2015 01:15 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: REQUIRED, 2.1: DONE

Backported into ruby_2_2 branch at r50293.

#5 - 04/13/2015 01:16 PM - usa (Usaku NAKAMURA)

- Backport changed from 1.9.3: REQUIRED, 2.0.0: REQUIRED, 2.1: DONE to 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: DONE

ruby_2_0_0 r50294 merged revision(s) 50292.

#6 - 04/28/2015 12:40 AM - terceiro (Antonio Terceiro)

- File CVE-2015-1855.patch added

Hi,

I was able to backport the patch to Ruby 1.9.3, and it will be included in a Debian wheezy security update soon. I am attaching the patch here.

Files

CVE-2015-1855.patch	12.5 KB	04/28/2015	terceiro (Antonio Terceiro)