Ruby master - Bug #4324

[ext/openssl] Parsing of incorrect ASN.1 values succeeds

01/26/2011 09:35 AM - MartinBosslet (Martin Bosslet)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:	1.9.3		
ruby -v:	trunk	**Backport:**	

Description

=begin
Hi,

I read about this bug of OpenSSL this morning: http://rt.openssl.org/Ticket/Display.html?id=2438
What struck me was the following sentence:

"The ASN1 parser should reject indefinite length primitive encodings as
that is illegal."

I tested whether Ruby (trunk) ASN.1 decoding was also affected:

```
require 'openssl'
require 'pp'

spec = %w{ 02 80 02 01 01 00 00 }
raw = [spec.join('')].pack('H*')
asn1 = OpenSSL::ASN1.decode(raw)
pp asn1
```

=>

#

This bug is a direct consequence of the bug in OpenSSL referred to above. Parsing
should fail in this case as primitive values cannot have an infinite length without
having the constructed bits set. (A correct encoding for the above would be this:
%w{ 22 80 02 01 01 00 00 }) But fortunately this is fixed quite easy.
By applying the appended patch, above script yields this exception:

=>

```
test.rb:6:in decode': Infinite length for primitive value (OpenSSL::ASN1::ASN1Error)
from test.rb:6:in'
```

Regards,
Martin
=end

Associated revisions

Revision 0522ffd5 - 01/26/2011 08:17 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl_asn1.c (ossl_asn1_decode0): OpenSSL::ASN1.decode should reject indefinite length primitive encodings as that is illegal. Patch by Martin Bosslet. See #4324.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@30656 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 30656 - 01/26/2011 08:17 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl_asn1.c (ossl_asn1_decode0): OpenSSL::ASN1.decode should reject indefinite length primitive encodings as that is illegal. Patch by Martin Bosslet. See #4324.

Revision 30656 - 01/26/2011 08:17 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl_asn1.c (ossl_asn1_decode0): OpenSSL::ASN1.decode should reject indefinite length primitive encodings as that is illegal. Patch by Martin Bosslet. See #4324.

Revision 30656 - 01/26/2011 08:17 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl_asn1.c (ossl_asn1_decode0): OpenSSL::ASN1.decode should reject indefinite length primitive encodings as that is illegal. Patch by Martin Bosslet. See #4324.

Revision 30656 - 01/26/2011 08:17 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl_asn1.c (ossl_asn1_decode0): OpenSSL::ASN1.decode should reject indefinite length primitive encodings as that is illegal. Patch by Martin Bosslet. See #4324.

Revision 30656 - 01/26/2011 08:17 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl_asn1.c (ossl_asn1_decode0): OpenSSL::ASN1.decode should reject indefinite length primitive encodings as that is illegal. Patch by Martin Bosslet. See #4324.

Revision 30656 - 01/26/2011 08:17 AM - nahi (Hiroshi Nakamura)

- ext/openssl/ossl_asn1.c (ossl_asn1_decode0): OpenSSL::ASN1.decode should reject indefinite length primitive encodings as that is illegal. Patch by Martin Bosslet. See #4324.

History

#1 - 01/26/2011 05:19 PM - nahi (Hiroshi Nakamura)

- Status changed from Open to Closed

=begin
Merged at r30656. Thanks.
=end

#2 - 01/26/2011 06:48 PM - mame (Yusuke Endoh)

=begin
Hi,

2011/1/26 Martin Bosslet redmine@ruby-lang.org:

> I read about this bug of OpenSSL this morning: http://rt.openssl.org/Ticket/Display.html?id=2438

Thank you for the information.
The URL seems to require authentification, but I managed to read it
by google:

http://rt.openssl.org/Ticket/Display.html?id=2438&user=guest&pass=guest

> What struck me was the following sentence:
>
> "The ASN1 parser should reject indefinite length primitive encodings as
> that is illegal."

I'm not sure that I understand the problem correctly.

ext/openssl (not openssl itself but Ruby binding) has its own ASN1
parser, and the parser does not follow the spec that openssl assumes
the users to follow, right?

--
Yusuke Endoh mame@tsg.ne.jp

=end

Files