# Ruby - Bug #3862

## Bugs in the OpenSSL extension on sparc64

09/23/2010 04:49 AM - jeremyevans0 (Jeremy Evans)

| | | | |
|---|---|---|---|
| **Status:** | Closed | | |
| **Priority:** | Normal | | |
| **Assignee:** | MartinBosslet (Martin Bosslet) | | |
| **Target version:** | | | |
| **ruby -v:** | - | **Backport:** | |

**Description**

=begin
The OpenSSL extension has some bugs on sparc64, either in the code or in the test suite. Here are the errors that are received when running the 1.9.2 test suite on sparc64 on OpenBSD:

1. Failure:
   test_decode(OpenSSL::TestASN1)
   [/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_asn1.rb:195]:
   <"\x8F\
   \xA8\f|\xD7JV\x92\b\xE9\xC1\xC5\x90\xEB\xB0\x9E!\x86\xD5\x8F\xAC\x7Fa\x1E<$\xD8_\xC9\x98\xABv\xC2[\x15\x97\xD6\xCA
   X\xAA\xB7\x12QK\x02c\xFE\xCF;(\x89Zm\xED0V
   +rQ\xED\x17/\xA8\xB2d\xABN\xDC\x1F\v\xC6\f\x10w\xA7\xFEd\xE1\xFA\x1E\x8C\xDB\xED\x97\xD0\xE1\xE6\xDDo\xFD\xFD\x
   FC~\xFE\xDF\xA8x{\x1C\xA4\x13\xF8E\x02\xB4\x1Ev\xF8\xDF
   +\xC3\x14$~\xD4\xE3t\xB2\xAF"\xF1?f\xB0yL"> expected but was
   <"\x9E*\xC8zH\xF0\xB8\xAA\xF4<\xFD\x81ud\xE6\x19\x87I\xAB\x8Du\xB9\xE0u\x94t\x87\x06\xDFb\xC2\x98\xBB9p\x88w\x84R
   3'\xBE\x84_\xD3\xF7\xDB\xDA\xE2\xD5\xD7\xE0?\x16#\x99
   +\xF1\xE8\x80I\x90\xCDic\r\x8A2\x8A\xA3\xC9\xB9\x92n\x04\n\x9C\xF5C\x95\xE0/\x8D\r{\xB3\xB0\xE0j\xCA\xE4\xDF\xC9\x88\
   x05\x88\xCE\x82\xB1\xE7\x13:}\xF7\x19\xCAG3\xAD\x
   +9F\xBC\xA7\xAD\xD3,\xE9\xD00\xDF\xA9P\x1F\x14\xA7I\x9B\xB3\x87m">.

2. Failure:
   test_create_by_factory(OpenSSL::TestX509Extension)
   [/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_x509ext.rb:41]:
   <"0\x12\x06\x03U\x1D\x13\x01\x01\x00\x04\b0\x06\x01\x01\x00\x02\x01\x02"> expected but was
   <"0\x12\x06\x03U\x1D\x13\x01\x01\xFF\x04\b0\x06\x01\x01\xFF\x02\x01\x02">.

3. Failure:
   test_new(OpenSSL::TestX509Extension)
   [/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_x509ext.rb:29]:
   expected but was
   .

4. Failure:
   test_attr(OpenSSL::TestX509Request)
   [/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_x509req.rb:94]:
   <[["keyUsage", "Digital Signature, Key Encipherment", true],
   ["subjectAltName", "email:gotoyuzo@ruby-lang.org", false]]> expected
   but was
   <[["keyUsage", "Digital Signature, Key Encipherment", false],
   ["subjectAltName", "email:gotoyuzo@ruby-lang.org", false]]>.

I spoke to Aaron Patterson about this and he wasn't sure if this is a bug in the test suite that should be made platform dependent, or if was a bug in the code.
=end

### History

**#1 - 09/23/2010 09:35 PM - naruse (Yui NARUSE)**

*- Status changed from Open to Assigned*

*- Assignee set to nahi (Hiroshi Nakamura)*

=begin

=end

#### #2 - 12/10/2010 03:59 AM - tenderlovemaking (Aaron Patterson)

*- Assignee changed from nahi (Hiroshi Nakamura) to tenderlovemaking (Aaron Patterson)*

=begin

=end

#### #3 - 12/26/2010 02:52 PM - naruse (Yui NARUSE)

*- Priority changed from Normal to 3*

=begin

=end

#### #4 - 06/11/2011 02:43 PM - ko1 (Koichi Sasada)

How about it?

#### #5 - 06/12/2011 05:25 AM - MartinBosslet (Martin Bosslet)

Hi,

Aaron, I could take this if you like?
I neither have OpenBSD nor sparc64, but I could analyze
the results and tell whether this is a real bug or what
else might have caused this behavior.

#### #6 - 06/12/2011 06:23 AM - tenderlovemaking (Aaron Patterson)

*- ruby -v changed from ruby 1.9.2p0 (2010-08-18 revision 29036) [sparc64-openbsd4.8] to -*

On Sun, Jun 12, 2011 at 05:25:35AM +0900, Martin Bosslet wrote:

> Issue #3862 has been updated by Martin Bosslet.
>
> Hi,
>
> Aaron, I could take this if you like?
> I neither have OpenBSD nor sparc64, but I could analyze
> the results and tell whether this is a real bug or what
> else might have caused this behavior.

Yes, please!  I haven't been able to get my hands on a sparc64 machine. :(

--
Aaron Patterson
http://tenderlovemaking.com/

#### #7 - 06/12/2011 11:06 PM - MartinBosslet (Martin Bosslet)

*- Assignee changed from tenderlovemaking (Aaron Patterson) to MartinBosslet (Martin Bosslet)*

Ok, I'll see what I can find out :)

#### #8 - 06/26/2011 08:14 AM - MartinBosslet (Martin Bosslet)

*- Status changed from Assigned to Feedback*

Jeremy Evans wrote:

> =begin
> The OpenSSL extension has some bugs on sparc64, either in the code or in the test suite.  Here are the errors that are received when running the 1.9.2 test suite on sparc64 on OpenBSD:
>
> 1. Failure:

test_create_by_factory(OpenSSL::TestX509Extension)
[/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_x509ext.rb:41]:
<"0\x12\x06\x03U\x1D\x13\x01\x01\x00\x04\b0\x06\x01\x01\x00\x02\x01\x02"> expected but was
<"0\x12\x06\x03U\x1D\x13\x01\x01\xFF\x04\b0\x06\x01\x01\xFF\x02\x01\x02">.

The former encoding is that of @basic_constraints in test_x509ext.rb.

It is defined as

```
@basic_constraints_value = OpenSSL::ASN1::Sequence([
OpenSSL::ASN1::Boolean(true),   # CA
OpenSSL::ASN1::Integer(2)       # pathlen
])
@basic_constraints = OpenSSL::ASN1::Sequence([
OpenSSL::ASN1::ObjectId("basicConstraints"),
OpenSSL::ASN1::Boolean(true),
OpenSSL::ASN1::OctetString(@basic_constraints_value.to_der),
])
```

Something must have gone wrong, either parsing OpenSSL::ASN1::Boolean(true) or encoding it again during #to_der because the encoding should be "\x01\x01\xFF" instead of "\x01\x01\x00".

1. Failure:
   test_new(OpenSSL::TestX509Extension)
   [/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_x509ext.rb:29]:
   expected but was
   .

Same cause as in 8), where "true" was expected the actual value is "false". Could have happened either in OpenSSL::X509::Extension#initialize or in @basic_constraints.to_der.

1. Failure:
   test_attr(OpenSSL::TestX509Request)
   [/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_x509req.rb:94]:
   <[["keyUsage", "Digital Signature, Key Encipherment", true],
   ["subjectAltName", "email:gotoyuzo@ruby-lang.org", false]]> expected
   but was
   <[["keyUsage", "Digital Signature, Key Encipherment", false],
   ["subjectAltName", "email:gotoyuzo@ruby-lang.org", false]]>.

It again seems that decoding a ASN.1 boolean "true" was wrongly decoded as "false" in the end. But I' can't tell whether this happened when encoding the attributes after creating them with OpenSSL::X509::ExtensionFactory#create_extension or when decoding them via OpenSSL::ASN1.decode.

1. Failure:
   test_decode(OpenSSL::TestASN1)
   [/usr/ports/pobj/ruby-1.9.2-p0/ruby-1.9.2-p0/test/openssl/test_asn1.rb:195]:
   <"\x8F\
   \xA8\f|\xD7JV\x92\b\xE9\xC1\xC5\x90\xEB\xB0\x9E!\x86\xD5\x8F\xAC\x7Fa\x1E<$\xD8_\xC9\x98\xABv\xC2[\x15\x97\xD6\xCAX\xAA\xB7\
   x12QK\x02c\xFE\xCF;(\x89Zm\xED0V
   +rQ\xED\x17/\xA8\xB2d\xABN\xDC\x1F\v\xC6\f\x10w\xA7\xFEd\xE1\xFA\x1E\x8C\xDB\xED\x97\xD0\xE1\xE6\xDDo\xFD\xFD\xFC~\xFE\x
   DF\xA8x{\x1C\xA4\x13\xF8E\x02\xB4\x1Ev\xF8\xDF
   +\xC3\x14$~\xD4\xE3t\xB2\xAF"\xF1?f\xB0yL"> expected but was
   <"\x9E*\xC8zH\xF0\xB8\xAA\xF4<\xFD\x81ud\xE6\x19\x87l\xAB\x8Du\xB9\xE0u\x94t\x87\x06\xDFb\xC2\x98\xBB9p\x88w\x84R3'\xBE\x84
   _\xD3\xF7\xDB\xDA\xE2\xD5\xD7\xE0?\x16#\x99
   +\xF1\xE8\x80l\x90\xCDic\r\x8A2\x8A\xA3\xC9\xB9\x92n\x04\n\x9C\xF5C\x95\xE0/\x8D\r{\xB3\xB0\xE0j\xCA\xE4\xDF\xC9\x88\x05\x88\xC
   E\x82\xB1\xE7\x13:}\xF7\x19\xCAG3\xAD\x
   +9F\xBC\xA7\xAD\xD3,\xE9\xD00\xDF\xA9P\x1F\x14\xA7l\x9B\xB3\x87m">.

My bet would be that this is also related to the obvious problems with ASN.1 booleans. The values being compared here are signatures on the DER encoding of a certificate. I assume that the encoding was already different due to the boolean problems and so the resulting signature would also be different.

It would help if I knew the exact OpenSSL version used that raised these failures.

Could this be related to r29075? Here is what it says in the change log:

- backport r29071 from ruby_1_8;

```
    * ext/openssl/ossl_asn1.c (obj_to_asn1bool): fixed ASN1::Boolean
      encoding issue for OpenSSL 1.0.0 compatibility.
```

```
ASN1::Boolean.new(false).to_der wrongly generated "\1\1\377" which
means 'true'.
```

```
ASN1_TYPE_set of OpenSSL <= 0.9.8 treats value 0x100 as 'false'
but OpenSSL >= 1.0.0 treats it as 'true'.  ruby-ossl was using
0x100 for 'false' for backward compatibility.  Just use 0x0 for
the case OpenSSL >= OpenSSL 0.9.7.
```

#### #9 - 06/28/2011 11:32 AM - jeremyevans0 (Jeremy Evans)

Based on the when I submitted this bug, I assume that the OpenSSL version was 0.9.8k (1.0.0a wasn't included in OpenBSD -current until 2010-10-01). If it would be helpful to get this retested with 1.0.0a, please let me know and I'll see if I can get another test done.

#### #10 - 06/28/2011 08:50 PM - MartinBosslet (Martin Bosslet)

Yes, I'd really appreciate your help there since I neither have access to OpenBSD nor sparc64 right now. It would be interesting to see whether you are able to reproduce these bugs with a trunk version of Ruby using OpenSSL 1.0.0. If not so, then I'd wonder if it were still reproducible with 0.9.8 (still with Ruby from trunk). That would help a lot, thanks already!

#### #11 - 06/29/2011 01:04 AM - jeremyevans0 (Jeremy Evans)

This appears to be fixed, running the following on OpenBSD-sparc64 -current works:

```
testrb test/openssl/test_*
Started
.....................................................................................
Finished in 15.489679 seconds.

92 tests, 1212 assertions, 0 failures, 0 errors, 0 skips
```

This is with 1.9.2p180, but I assume this is the same in ruby-head. My guess is the update to OpenSSL 1.0.0a fixed it. It should be safe to close this issue now.

#### #12 - 06/29/2011 02:54 AM - MartinBosslet (Martin Bosslet)

*- Category changed from lib to ext*

*- Status changed from Feedback to Closed*

Great! Thanks, Jeremy, for investigating the issue!

### Files

| | | | |
|---|---|---|---|
| noname | 500 Bytes | 06/12/2011 | tenderlovemaking (Aaron Patterson) |