Ruby master - Bug #6134

Ruby crashes when calling OpenSSL::PKCS7.new with invalid PKCS7 data

03/13/2012 01:44 AM - mattv (Matt Venables)

Status:	Closed		
Priority:	Normal		
Assignee:	MartinBosslet (Martin Bosslet)		
Target version:	1.9.3		
ruby -v:	ruby 1.9.3p125 (2012-02-16 revision 34643) [x86_64-darwin11.3.0]	**Backport:**	

Description

Reproducing steps:
Run the following script in 1.9.3-p125 (it is attached to the issue as well)

```
require 'openssl'
contents = File.read(FILE)
begin
OpenSSL::PKCS7.new(contents)
puts "OK"
rescue => e
puts "Error!"
puts e
end
```

Expected Result:
Ruby should not crash, the exception should be caught, and the script should output:
"Error!" followed by the exception ("Could not parse the PKCS7: ...")

Actual Result:
The script outputs "Error!" followed by the exception, and ruby segfaults. (Crash report attached).
The script occasionally operates as expected, but running it 3 or 4 times will always yield the segmentation fault.

This only happens in 1.9.3 (1.9.2 is working fine).

Tested on:
1.9.3-p0 (ruby 1.9.3p0 (2011-10-30 revision 33570) [x86_64-darwin11.3.0])
1.9.3-p125 (ruby 1.9.3p125 (2012-02-16 revision 34643) [x86_64-darwin11.3.0])
1.9.3-head (ruby 1.9.3p163 (2012-03-06 revision 34932) [x86_64-darwin11.3.0])

Associated revisions

Revision aad347f5 - 03/29/2012 01:27 AM - emboss

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.
- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@35167 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 35167 - 03/29/2012 01:27 AM - emboss

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.
- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

Revision 35167 - 03/29/2012 01:27 AM - emboss

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.
- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

Revision 35167 - 03/29/2012 01:27 AM - emboss

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.

- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

Revision 35167 - 03/29/2012 01:27 AM - emboss

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.
- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

Revision 35167 - 03/29/2012 01:27 AM - emboss

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.
- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

Revision 35167 - 03/29/2012 01:27 AM - emboss

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.
- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

Revision 7d8e27a6 - 03/30/2012 05:17 AM - naruse (Yui NARUSE)

merge revision(s) 35162,35167: [Backport #6220]

```
    * test/openssl/test_x509cert.rb: Exclude test that fails when issuing
      a certificate with RSA signature and DSS1 digest for earlier
      OpenSSL versions when used in conjunction with OpenSSL 1.0.1.
      Thanks, Vit Ondruch, for reporting the issue.
      [ruby-core:42949][Bug #6089]

    * ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.

    * test/openssl/test_pkcs7.rb: assert correct behavior for it.
      Thanks to Matt Venables for reporting the issue.
      [ruby-core:43250][Bug #6134]

    * test/openssl/test_x509cert.rb: exclude test that fails when issuing
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@35179 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 03/13/2012 05:35 AM - MartinBosslet (Martin Bosslet)

- Category set to ext

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

- Target version set to 1.9.3

Thank you for reporting this issue. Could you please verify that your (native) OpenSSL library has not been upgraded in the meantime? If it was, could you please additionally check if the problem still does not occur when using a re-installed 1.9.2 with this newer version of OpenSSL? Thanks,

-Martin

#2 - 03/13/2012 10:34 PM - mattv (Matt Venables)

I don't believe OpenSSL has been upgraded, but, running "openssl version" gives me:
OpenSSL 0.9.8r 8 Feb 2011

I reinstalled 1.9.2-p318 (and 1.9.2-p180) and everything worked as expected (same as before - no segfault). I then reinstalled 1.9.3-p125 and 1.9.3-head (p163) and had the same segfault on both versions.

For completeness, I tried the same code on a clean Ubuntu install (Ubuntu 11.10 codename oneiric) with the exact same results (1.9.2 passes, 1.9.3-p125 and 1.9.3-head both segfault)

openssl version: OpenSSL 1.0.0e 6 Sep 2011
ruby 1.9.2 version (PASS): ruby 1.9.2p290 (2011-07-09 revision 32553) [x86_64-linux]
ruby 1.9.3 version (SEGFAULT): ruby 1.9.3p125 (2012-02-16 revision 34643) [x86_64-linux]
ruby 1.9.3-head version (SEGFAULT): ruby 1.9.3p163 (2012-03-06 revision 34932) [x86_64-linux]

Another thing worth noting - if the test script was modified to use valid PKCS7 data, the script passes on all systems. It only segfaults when invalid data is used.

#3 - 03/14/2012 01:44 AM - MartinBosslet (Martin Bosslet)

Alright, so it is caused by something in 1.9.3. Thanks, that already helps a lot!

#4 - 03/29/2012 10:27 AM - Anonymous

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r35167.
Matt, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/openssl/ossl_pkcs7.c: fix crash when parsing garbage data.
- test/openssl/test_pkcs7.rb: assert correct behavior for it. Thanks to Matt Venables for reporting the issue. [ruby-core:43250][Bug #6134]

Files

openssl-pkcs7-bug.rb	139 Bytes	03/13/2012	mattv (Matt Venables)
ruby_2012-03-12-123740_Matt-Venables-Macbook-Pro.crash	10.2 KB	03/13/2012	mattv (Matt Venables)