

## Ruby trunk - Bug #9743

### memory leak in openssl ossl\_pkey\_verify leaks memory

04/15/2014 09:57 AM - tux (Joel Westerberg)

<b>Status:</b> Closed	
<b>Priority:</b> Normal	
<b>Assignee:</b> zzak (Zachary Scott)	
<b>Target version:</b>	
<b>ruby -v:</b> 2.2.0	<b>Backport:</b> 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: DONE
<b>Description</b> repeated calls to <code>pub_key.verify(digest, signature, data)</code> leaks memory.  from what I can gather from the openssl documentation, there seems to be a missing call to <code>EVP_MD_CTX_cleanup()</code>  FILE: <code>ossl_pkey.c</code>  <pre>326     EVP_VerifyUpdate(&amp;ctx, RSTRING_PTR(data), RSTRING_LEN(data)); 327     switch (EVP_VerifyFinal(&amp;ctx, (unsigned char *)RSTRING_PTR(sig), RSTRING_LENINT(sig), pkey)) { 328     case 0:</pre> from the openssl docs:  <a href="http://www.openssl.org/docs/crypto/EVP_VerifyInit.html">http://www.openssl.org/docs/crypto/EVP_VerifyInit.html</a>  The call to <code>EVP_VerifyFinal()</code> internally finalizes a copy of the digest context. This means that calls to <code>EVP_VerifyUpdate()</code> and <code>EVP_VerifyFinal()</code> can be called later to digest and verify additional data. Since only a copy of the digest context is ever finalized the context must be cleaned up after use by calling <code>EVP_MD_CTX_cleanup()</code> or a memory leak will occur.	
<b>Related issues:</b>	
Related to Backport200 - Backport #9746: backport r45595	<b>Closed</b> <b>04/16/2014</b>
Related to Ruby trunk - Bug #9984: OpenSSL::TestPKeyRSA#test_sign_verify_memo...	<b>Closed</b> <b>06/27/2014</b>

#### Associated revisions

##### Revision a39b88d2 - 04/16/2014 12:51 AM - nobu (Nobuyoshi Nakada)

`ossl_pkey.c`: fix memory leak

- `ext/openssl/ossl_pkey.c (ossl_pkey_verify)`: as `EVP_VerifyFinal()` finalizes only a copy of the digest context, the context must be cleaned up after initialization by `EVP_MD_CTX_cleanup()` or a memory leak will occur. [ruby-core:62038] [Bug #9743]

git-svn-id: [svn+ssh://ci.ruby-lang.org/ruby/trunk@45595](https://ci.ruby-lang.org/ruby/trunk@45595) b2dd03c8-39d4-4d8f-98ff-823fe69b080e

##### Revision 45595 - 04/16/2014 12:51 AM - nobu (Nobuyoshi Nakada)

`ossl_pkey.c`: fix memory leak

- `ext/openssl/ossl_pkey.c (ossl_pkey_verify)`: as `EVP_VerifyFinal()` finalizes only a copy of the digest context, the context must be cleaned up after initialization by `EVP_MD_CTX_cleanup()` or a memory leak will occur. [ruby-core:62038] [Bug #9743]

**Revision 45595 - 04/16/2014 12:51 AM - nobu (Nobuyoshi Nakada)**

ossl\_pkey.c: fix memory leak

- ext/openssl/ossl\_pkey.c (ossl\_pkey\_verify): as EVP\_VerifyFinal() finalizes only a copy of the digest context, the context must be cleaned up after initialization by EVP\_MD\_CTX\_cleanup() or a memory leak will occur. [ruby-core:62038] [Bug #9743]

**Revision 45595 - 04/16/2014 12:51 AM - nobu (Nobuyoshi Nakada)**

ossl\_pkey.c: fix memory leak

- ext/openssl/ossl\_pkey.c (ossl\_pkey\_verify): as EVP\_VerifyFinal() finalizes only a copy of the digest context, the context must be cleaned up after initialization by EVP\_MD\_CTX\_cleanup() or a memory leak will occur. [ruby-core:62038] [Bug #9743]

**Revision 45595 - 04/16/2014 12:51 AM - nobu (Nobuyoshi Nakada)**

ossl\_pkey.c: fix memory leak

- ext/openssl/ossl\_pkey.c (ossl\_pkey\_verify): as EVP\_VerifyFinal() finalizes only a copy of the digest context, the context must be cleaned up after initialization by EVP\_MD\_CTX\_cleanup() or a memory leak will occur. [ruby-core:62038] [Bug #9743]

**Revision 45595 - 04/16/2014 12:51 AM - nobu (Nobuyoshi Nakada)**

ossl\_pkey.c: fix memory leak

- ext/openssl/ossl\_pkey.c (ossl\_pkey\_verify): as EVP\_VerifyFinal() finalizes only a copy of the digest context, the context must be cleaned up after initialization by EVP\_MD\_CTX\_cleanup() or a memory leak will occur. [ruby-core:62038] [Bug #9743]

**Revision 01cf2127 - 05/04/2014 05:44 PM - nagachika (Tomoyuki Chikanaga)**

merge revision(s) r45595: [Backport #9743] [Backport #9745]

```
* ext/openssl/ossl_pkey.c (ossl_pkey_verify): as EVP_VerifyFinal()
finalizes only a copy of the digest context, the context must be
cleaned up after initialization by EVP_MD_CTX_cleanup() or a
memory leak will occur. [ruby-core:62038] [Bug #9743]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby\_2\_1@45821 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

**Revision 45821 - 05/04/2014 05:44 PM - nagachika (Tomoyuki Chikanaga)**

merge revision(s) r45595: [Backport #9743] [Backport #9745]

```
* ext/openssl/ossl_pkey.c (ossl_pkey_verify): as EVP_VerifyFinal()
finalizes only a copy of the digest context, the context must be
cleaned up after initialization by EVP_MD_CTX_cleanup() or a
memory leak will occur. [ruby-core:62038] [Bug #9743]
```

**Revision b786887a - 05/07/2014 04:59 PM - usa (Usaku NAKAMURA)**

merge revision(s) 45595: [Backport #9743]

```
* ext/openssl/openssl_pkey.c (openssl_pkey_verify): as EVP_VerifyFinal()
finalizes only a copy of the digest context, the context must be
cleaned up after initialization by EVP_MD_CTX_cleanup() or a
memory leak will occur. [ruby-core:62038] [Bug #9743]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby\_2\_0\_0@45868 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

**Revision 45868 - 05/07/2014 04:59 PM - usa (Usaku NAKAMURA)**

merge revision(s) 45595: [Backport #9743]

```
* ext/openssl/openssl_pkey.c (openssl_pkey_verify): as EVP_VerifyFinal()
finalizes only a copy of the digest context, the context must be
cleaned up after initialization by EVP_MD_CTX_cleanup() or a
memory leak will occur. [ruby-core:62038] [Bug #9743]
```

**History**

---

**#1 - 04/16/2014 12:51 AM - nobu (Nobuyoshi Nakada)**

- Status changed from Open to Closed
- % Done changed from 0 to 100

Applied in changeset [r45595](#).

---

openssl\_pkey.c: fix memory leak

- ext/openssl/openssl\_pkey.c (openssl\_pkey\_verify): as EVP\_VerifyFinal() finalizes only a copy of the digest context, the context must be cleaned up after initialization by EVP\_MD\_CTX\_cleanup() or a memory leak will occur. [Bug [#9743](#)]

**#2 - 04/16/2014 12:56 AM - nobu (Nobuyoshi Nakada)**

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

**#3 - 05/04/2014 05:45 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

[r45595](#) was backported into ruby\_2\_1 at r45821.

**#4 - 05/07/2014 05:00 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*

backported into ruby\_2\_0\_0 at r45868.

**#5 - 05/07/2014 05:13 PM - usa (Usaku NAKAMURA)**

- Related to Backport #9746: backport r45595 added

**#6 - 06/26/2014 08:38 AM - vo.x (Vit Ondruch)**

This is causing test suite timeout on Fedora Rawhide ARM builder :/

<https://kojipkgs.fedoraproject.org/work/tasks/4012/7074012/build.log>

**#7 - 06/27/2014 10:48 AM - vo.x (Vit Ondruch)**

- Related to Bug #9984: *OpenSSL::TestPKeyRSA#test\_sign\_verify\_memory\_leak* timeouts on ARM added

**#8 - 01/28/2015 06:15 AM - zzak (Zachary Scott)**

- Status changed from *Closed* to *Open*

- Assignee set to zzak (Zachary Scott)

- ruby -v changed from 2.1.1 to 2.2.0

Seeing this test failure on travis:

<https://travis-ci.org/zzak/openssl/jobs/48587976>

I think we should re-open this ticket until its resolved.

**#9 - 06/03/2015 05:11 PM - zzak (Zachary Scott)**

- Status changed from *Open* to *Closed*

The failure has been fixed, so we can close this ticket.