

Ruby master - Bug #9743

memory leak in openssl ossl_pkey_verify leaks memory

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

Status: Closed	
Priority: Normal	
Assignee: zzak (Zachary Scott)	
Target version:	
ruby -v: 2.2.0	Backport: 1.9.3: REQUIRED, 2.0.0: DONE, 2.1: DONE
Description 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(&ctx, RSTRING_PTR(data), RSTRING_LEN(data)); 327 switch (EVP_VerifyFinal(&ctx, (unsigned char *)RSTRING_PTR(sig), RSTRING_LENINT(sig), pkey)) { 328 case 0:</pre> from the openssl docs: http://www.openssl.org/docs/crypto/EVP_VerifyInit.html 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.	
Related issues:	
Related to Backport200 - Backport #9746: backport r45595	Closed 04/16/2014
Related to Ruby master - Bug #9984: OpenSSL::TestPKeyRSA#test_sign_verify_mem...	Closed 06/27/2014

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/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]

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

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. [ruby-core:62038] [Bug #9743]

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

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. [ruby-core:62038] [Bug #9743]

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

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. [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/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_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/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]
```

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. [ruby-core:62038] [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.