Ruby master - Bug #10735

Memory leak in openssl ossl_pkey_sign

01/12/2015 06:09 PM - viktor (Viktor Vasilev)

Status:	Closed		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	ruby 1.9.3p484 (2013-11-22 revision 43786) [x86_64-linux]	**Backport:**	2.0.0: REQUIRED, 2.1: DONE, 2.2: DONE

Description

Similar to the memory leak fixed in https://bugs.ruby-lang.org/issues/9743 there is an issue with ossl_pkey_sign. The ruby heap usage reported through GC.stat remains very stable, while the process heap grows linearly with the number of OpenSSL::PKey::RSA sign calls.
The documentation at https://www.openssl.org/docs/crypto/EVP_SignInit.html (similar to EVP_VerifyInit) mentions that not disposing the context causes a leak.

To reproduce: https://gist.github.com/viktorium/f032cdc8906f43dac94e
A patch with a fix very similar to issue #9743: https://gist.github.com/viktorium/b466b72c83d2ab90182c

Associated revisions

Revision 85dd19cf - 11/13/2015 05:01 AM - zzak (Zachary Scott)

- ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@52556 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 52556 - 11/13/2015 05:01 AM - zzak (Zachary Scott)

- ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]

Revision 52556 - 11/13/2015 05:01 AM - zzak (Zachary Scott)

- ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]

Revision 52556 - 11/13/2015 05:01 AM - zzak (Zachary Scott)

- ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]

Revision 52556 - 11/13/2015 05:01 AM - zzak (Zachary Scott)

- ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]

Revision 52556 - 11/13/2015 05:01 AM - zzak (Zachary Scott)

- ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]

Revision dacb9169 - 11/18/2015 11:39 AM - usa (Usaku NAKAMURA)

merge revision(s) 52556,52557: [Backport #10735]

```
    * ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_1@52643 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 52643 - 11/18/2015 11:39 AM - usa (Usaku NAKAMURA)

merge revision(s) 52556,52557: [Backport #10735]

```
* ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]
```

Revision bd210ff1 - 11/18/2015 03:37 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52556,52557: [Backport #10735]

```
    * ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@52651 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 52651 - 11/18/2015 03:37 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52556,52557: [Backport #10735]

```
* ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]
```

Revision 478cdf49 - 11/18/2015 03:49 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52016,52017,52019,52020,52021: [Backport #10735]

```
    * enc/euc_jp.c (mbc_case_fold): check given string is valid or not,
      and if invalid, return 1. [Bug #11486]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_2_2@52652 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 52652 - 11/18/2015 03:49 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 52016,52017,52019,52020,52021: [Backport #10735]

```
* enc/euc_jp.c (mbc_case_fold): check given string is valid or not,
  and if invalid, return 1. [Bug #11486]
```

History

#1 - 01/12/2015 07:20 PM - zzak (Zachary Scott)

- Status changed from Open to Assigned

- Assignee set to zzak (Zachary Scott)

I know you tried this with 1.9.3, but could you try to repro on trunk (and newer rubies) first?

1.9.3 will be EOL soon, and I want to make sure we fix it upstream before attempting any backports

#2 - 01/12/2015 07:21 PM - zzak (Zachary Scott)

- Assignee changed from zzak (Zachary Scott) to openssl

- Priority changed from 5 to Normal

#3 - 01/12/2015 09:12 PM - viktor (Viktor Vasilev)

Zachary Scott wrote:

> I know you tried this with 1.9.3, but could you try to repro on trunk (and newer rubies) first?
>
> 1.9.3 will be EOL soon, and I want to make sure we fix it upstream before attempting any backports

Hi Zachary,

Just ran the test case against Ruby 2.3.0dev (2015-01-12 trunk 49226) [x86_64-darwin14] and see the exact same memory leak:

```
{:count=>7, :heap_allocated_pages=>74, :heap_sorted_length=>75, :heap_allocatable_pages=>0, :heap_available_sl
ots=>30161, :heap_live_slots=>29720, :heap_free_slots=>441, :heap_final_slots=>0, :heap_marked_slots=>11592, :
heap_swept_slots=>10966, :heap_eden_pages=>74, :heap_tomb_pages=>0, :total_allocated_pages=>74, :total_freed_p
ages=>0, :total_allocated_objects=>91749, :total_freed_objects=>62029, :malloc_increase_bytes=>530256, :malloc
_increase_bytes_limit=>16777216, :minor_gc_count=>5, :major_gc_count=>2, :remembered_wb_unprotected_objects=>1
80, :remembered_wb_unprotected_objects_limit=>278, :old_objects=>10540, :old_objects_limit=>10818, :oldmalloc_
increase_bytes=>1808128, :oldmalloc_increase_bytes_limit=>16777216}
Memory 11736KB
```

<< 100_000 iterations of RSA sign >>

```
{:count=>25, :heap_allocated_pages=>74, :heap_sorted_length=>75, :heap_allocatable_pages=>0, :heap_available_s
lots=>30161, :heap_live_slots=>30108, :heap_free_slots=>53, :heap_final_slots=>0, :heap_marked_slots=>13570, :
heap_swept_slots=>11362, :heap_eden_pages=>74, :heap_tomb_pages=>0, :total_allocated_pages=>74, :total_freed_p
ages=>0, :total_allocated_objects=>392910, :total_freed_objects=>362802, :malloc_increase_bytes=>15616, :mallo
```

```
c_increase_bytes_limit=>16777216, :minor_gc_count=>22, :major_gc_count=>3, :remembered_wb_unprotected_objects=
>298, :remembered_wb_unprotected_objects_limit=>596, :old_objects=>13151, :old_objects_limit=>26046, :oldmallo
c_increase_bytes=>39904, :oldmalloc_increase_bytes_limit=>16777216}
Memory 26244KB
```

Let me know if I can provide further information.

#4 - 01/22/2015 09:22 AM - tonci (Tonči Damjanić)

Confirming the same with the current Ruby 2.2 (ruby 2.2.0p0 (2014-12-25 revision 49005) [x86_64-darwin14]):

```
{:count=>5, :heap_allocated_pages=>74, :heap_sorted_length=>75, :heap_allocatable_pages=>0, :heap_available_sl
ots=>30164, :heap_live_slots=>29039, :heap_free_slots=>1125, :heap_final_slots=>0, :heap_marked_slots=>8424, :
heap_swept_slots=>9725, :heap_eden_pages=>73, :heap_tomb_pages=>1, :total_allocated_pages=>74, :total_freed_pa
ges=>0, :total_allocated_objects=>52920, :total_freed_objects=>23881, :malloc_increase_bytes=>275968, :malloc_
increase_bytes_limit=>16777216, :minor_gc_count=>3, :major_gc_count=>2, :remembered_wb_unprotected_objects=>16
1, :remembered_wb_unprotected_objects_limit=>278, :old_objects=>8196, :old_objects_limit=>10808, :oldmalloc_in
crease_bytes=>276352, :oldmalloc_increase_bytes_limit=>16777216}
Memory 10188KB
```

100k iterations later:

```
{:count=>20, :heap_allocated_pages=>74, :heap_sorted_length=>75, :heap_allocatable_pages=>0, :heap_available_s
lots=>30164, :heap_live_slots=>29999, :heap_free_slots=>165, :heap_final_slots=>0, :heap_marked_slots=>9656, :
heap_swept_slots=>406, :heap_eden_pages=>74, :heap_tomb_pages=>0, :total_allocated_pages=>74, :total_freed_pag
es=>0, :total_allocated_objects=>353037, :total_freed_objects=>323038, :malloc_increase_bytes=>24000, :malloc_
increase_bytes_limit=>16777216, :minor_gc_count=>18, :major_gc_count=>2, :remembered_wb_unprotected_objects=>2
27, :remembered_wb_unprotected_objects_limit=>278, :old_objects=>9331, :old_objects_limit=>10808, :oldmalloc_i
ncrease_bytes=>1983872, :oldmalloc_increase_bytes_limit=>16777216}
Memory 25340KB
```

#5 - 04/13/2015 11:37 PM - zzak (Zachary Scott)

I've applied the patch to a branch, if you're on Ruby 2.2 you can try it out by adding this to your Gemfile:

gem "openssl", github: "ruby/openssl", branch: "ruby-bug-10735"

#6 - 11/13/2015 05:01 AM - zzak (Zachary Scott)

- Status changed from Assigned to Closed

Applied in changeset r52556.

- ext/openssl/ossl_pkey.c: Merge ruby/openssl@b9ea8ef [Bug #10735]

#7 - 11/13/2015 10:35 AM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.0.0: UNKNOWN, 2.1: UNKNOWN, 2.2: UNKNOWN to 2.0.0: REQUIRED, 2.1: REQUIRED, 2.2: REQUIRED

#8 - 11/18/2015 11:39 AM - usa (Usaku NAKAMURA)

- Backport changed from 2.0.0: REQUIRED, 2.1: REQUIRED, 2.2: REQUIRED to 2.0.0: REQUIRED, 2.1: DONE, 2.2: REQUIRED

ruby_2_1 r52643 merged revision(s) 52556,52557.

#9 - 11/18/2015 03:38 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.0.0: REQUIRED, 2.1: DONE, 2.2: REQUIRED to 2.0.0: REQUIRED, 2.1: DONE, 2.2: DONE

Backported into ruby_2_2 branch at r52651.