Backport191 - Bug #3000

Open SSL Segfaults

03/24/2010 06:20 AM - docwhat (Christian Höltje)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	1.9.1-p376	

Description

=begin
According the OpenSSL docs, we need to set the store->ex_data.sk to NULL before doing a verify on an x509 store.

See the attached patch. It's a simple change and prevents segfaults or undefined behavior when using SSL. This is probably a security problem, but I don't know enough to figure out how to exploit it.

The patch applies to the latest 1.9.1 as well as the p243 it was written for.
=end

Related issues:

Related to Ruby trunk - Bug #3817: current ruby-openssl impl wrongly utilizes...	**Closed**

History

#1 - 03/24/2010 06:30 AM - docwhat (Christian Höltje)

=begin
Okay, I thought this seemed familiar....

bug #1678 and bug #405 are also the same problem. This should really be fixed. It is a simple fix and has potential security issues.
=end

#2 - 03/25/2010 12:14 PM - nahi (Hiroshi Nakamura)

=begin
Hi,

On Wed, Mar 24, 2010 at 06:20, Christian Höltje redmine@ruby-lang.org wrote:

> According the OpenSSL docs, we need to set the store->ex_data.sk to NULL before doing a verify on an x509 store.

Would you please point an URL of the above document? I cannot find it...

I think that current ruby-openssl impl wrongly utilizes CRYPTO_EX_DATA
in X509_STORE
(I'm not talking about one in X509_STORE_*CTX*) and it requires fixes
a little bit more.

Regards,
// NaHi

=end

#3 - 03/26/2010 10:56 PM - mame (Yusuke Endoh)

=begin
Hi,

2010/3/25 NAKAMURA, Hiroshi nakahiro@gmail.com:

> On Wed, Mar 24, 2010 at 06:20, Christian Holtje redmine@ruby-lang.org wrote:
>
> > According the OpenSSL docs, we need to set the store->ex_data.sk to NULL before doing a verify on an x509 store.
>
> Would you please point an URL of the above document? I cannot find it...

Me too.

But, I confirmed that CRYPTO_set_ex_data actually dereferences the field ex_data.sk in the following version of openssl:

0.9.6a / 0.9.7a / 0.9.8a / 0.9.8j-n / 1.0.0-beta5

Though I cannot determine whether it is in ruby-openssl or openssl itself, there is certainly a bug.

I'll commit Christian's patch soon. Thanks!

--
Yusuke ENDOH mame@tsg.ne.jp

=end

#4 - 03/26/2010 11:07 PM - nahi (Hiroshi Nakamura)

=begin
Hi,

On Fri, Mar 26, 2010 at 22:56, Yusuke ENDOH mame@tsg.ne.jp wrote:

> Though I cannot determine whether it is in ruby-openssl or openssl itself, there is certainly a bug.

Yes.

> I'll commit Christian's patch soon. Thanks!

It's OK for a few days workaround. Please don't mind when I'll revert the "fix" later.

Regards,
// NaHi

=end

#5 - 03/26/2010 11:12 PM - mame (Yusuke Endoh)

=begin
Hi,

2010/3/26 NAKAMURA, Hiroshi nakahiro@gmail.com:

> On Fri, Mar 26, 2010 at 22:56, Yusuke ENDOH mame@tsg.ne.jp wrote:
>
> > Though I cannot determine whether it is in ruby-openssl or openssl itself, there is certainly a bug.
>
> Yes.
>
> > I'll commit Christian's patch soon. Thanks!
>
> It's OK for a few days workaround. Please don't mind when I'll revert the "fix" later.

Sure!

BTW, why don't you become a maintainer of ruby-openssl?
I guess you're eligible.

--
Yusuke ENDOH mame@tsg.ne.jp

=end

#6 - 03/28/2010 12:08 AM - mame (Yusuke Endoh)

- Status changed from Open to Closed

=begin
Applied at r27064. Thank you!
=end

#7 - 03/28/2010 06:38 AM - nahi (Hiroshi Nakamura)

=begin
It would be better off waiting for Christian's response.

Would you please reopen this ticket, Yusuke?
=end

#8 - 03/28/2010 12:44 PM - mame (Yusuke Endoh)

=begin
Hi,

2010/3/28 Hiroshi NAKAMURA redmine@ruby-lang.org:

> It would be better off waiting for Christian's response.

When you revert the patch, he can complain if he is not satisfied
with the revert.
But I believe Christian will not complain about how to fix, unless
SEGV occurs.

> Would you please reopen this ticket, Yusuke?

In terms of release management, I don't want to leave bug ticket
open just because of such a confirmation.

And I guess it is better for you to register a new ticket for your
concern of [ruby-core:28969] with the detail description.

--
Yusuke ENDOH mame@tsg.ne.jp

=end

#9 - 03/28/2010 01:42 PM - nahi (Hiroshi Nakamura)

=begin
Hi,

On Sun, Mar 28, 2010 at 12:44, Yusuke ENDOH mame@tsg.ne.jp wrote:

> > It would be better off waiting for Christian's response.
>
> When you revert the patch, he can complain if he is not satisfied
> with the revert.
> But I believe Christian will not complain about how to fix, unless
> SEGV occurs.

I'm not waiting for the confirmation. I'm asking Christian for
guessing how the "fix" you committed is correct.

> > Would you please reopen this ticket, Yusuke?
>
> In terms of release management, I don't want to leave bug ticket
> open just because of such a confirmation.

Closing a ticket too soon generally is not good for release management
I think. But I'm not a member of 1.9.1 development so it's your
business.

I don't think it should be done but you can close these tickets as well:
http://redmine.ruby-lang.org/issues/show/3000

http://redmine.ruby-lang.org/issues/show/2596
http://redmine.ruby-lang.org/issues/show/1678
http://redmine.ruby-lang.org/issues/show/1142
http://redmine.ruby-lang.org/issues/show/405

Regards,
// NaHi

=end

#10 - 03/28/2010 04:43 PM - mame (Yusuke Endoh)

=begin
Hi,

2010/3/28 NAKAMURA, Hiroshi nakahiro@gmail.com:

> On Sun, Mar 28, 2010 at 12:44, Yusuke ENDOH mame@tsg.ne.jp wrote:
>
> > It would be better off waiting for Christian's response.
>
> When you revert the patch, he can complain if he is not satisfied
> with the revert.
> But I believe Christian will not complain about how to fix, unless
> SEGV occurs.
>
> I'm not waiting for the confirmation. I'm asking Christian for
> guessing how the "fix" you committed is correct.

I cannot get your point.
I just commited the patch written by Christian himself. Why
do we need his guessing?

> > Would you please reopen this ticket, Yusuke?
>
> In terms of release management, I don't want to leave bug ticket
> open just because of such a confirmation.
>
> Closing a ticket too soon generally is not good for release management
> I think. But I'm not a member of 1.9.1 development so it's your
> business.

Currently, there is a convention that a ticket is closed when
a commit is done.
In fact, redmine even has an automatic mechanism that closes
ticket when any committer writes ML reference to ChangeLog in
trunk. (The mechanism does not work sometimes, though.)

It is good to discuss the convention, but I prefer the current
one.

Indeed, it is better to ask original poster to confirm whether
his/her issue is actually solved or not before closing tickets.
But it requires human-resource to manage tickets. We cannot
afford to do so.

> I don't think it should be done but you can close these tickets as well:
> http://redmine.ruby-lang.org/issues/show/3000
> http://redmine.ruby-lang.org/issues/show/2596
> http://redmine.ruby-lang.org/issues/show/1678
> http://redmine.ruby-lang.org/issues/show/1142
> http://redmine.ruby-lang.org/issues/show/405

Thank you. I couldn't identify some of these tickets.

- #3000 and #1678 are already closed.
- I'm not sure whether #2596 is really the same problem. I'll close it later unless there is objection.
- #1142 needs backport to ruby_1_9_1.

- #405 needs backport to ruby_1_8_7.

--
Yusuke ENDOH mame@tsg.ne.jp

=end

#11 - 03/28/2010 05:54 PM - nahi (Hiroshi Nakamura)

=begin
Hi,

On Sun, Mar 28, 2010 at 16:43, Yusuke ENDOH mame@tsg.ne.jp wrote:

> When you revert the patch, he can complain if he is not satisfied
> with the revert.
> But I believe Christian will not complain about how to fix, unless
> SEGV occurs.

> I'm not waiting for the confirmation. I'm asking Christian for
> guessing how the "fix" you committed is correct.

> I cannot get your point.
> I just commited the patch written by Christian himself. Why
> do we need his guessing?

Not by the reporter. I thought we should know how the "fix" is correct (or not.) But I've now understood that you closed the ticket for the fact that you've applied the patch by contributor. I think it's OK for you.

> Closing a ticket too soon generally is not good for release management
> I think. But I'm not a member of 1.9.1 development so it's your
> business.

> Currently, there is a convention that a ticket is closed when
> a commit is done.

Thanks for the explanation. But I wasn't talking about the point about confirmation by a reporter. There's a ticket that the cause is not fully identified yet but someone closed the ticket with a applying a workaround patch while I was digging into it by asking the reporter. I said it's not good about this point.

Regards,
// NaHi

=end

#12 - 03/28/2010 09:24 PM - mame (Yusuke Endoh)

=begin
Hi,

2010/3/28 NAKAMURA, Hiroshi nakahiro@gmail.com:

> There's a ticket that the cause is
> not fully identified yet but someone closed the ticket with a applying
> a workaround patch while I was digging into it by asking the reporter.

Aha, I understand what you mean.

There was certainly a bug at hand. And I thought the patch worked out the bug in the short term. So I committed it and closed this ticket.

Indeed, the patch may be formally wrong. The patch might be poking undocumented feature or bug of openssl. As you said, ruby-openssl might need major revamping including its design.

However, such document investigation and major revamping take cost.
Because there is no maintainer for ruby-openssl, we can't help but
do superficial fix, unfortunately.

Hiroshi, please think about becoming maintainer for openssl. It
will make everybody happy :-)

--
Yusuke ENDOH mame@tsg.ne.jp

=end

#13 - 03/29/2010 03:32 PM - nahi (Hiroshi Nakamura)

=begin
Hi,

On Sun, Mar 28, 2010 at 21:24, Yusuke ENDOH mame@tsg.ne.jp wrote:

> There's a ticket that the cause is
> not fully identified yet but someone closed the ticket with a applying
> a workaround patch while I was digging into it by asking the reporter.

There was certainly a bug at hand. And I thought the patch worked
out the bug in the short term. So I committed it and closed this
ticket.

Indeed, the patch may be formally wrong. The patch might be poking
undocumented feature or bug of openssl. As you said, ruby-openssl
might need major revamping including its design.

However, such document investigation and major revamping take cost.
Because there is no maintainer for ruby-openssl, we can't help but
do superficial fix, unfortunately.

The problem, for me, was closing the ticket without giving a time to
identify the cost for fix. Applying the workaround patch is OK. You
could have waited a response as I wrote in [ruby-core:29074].

> Hiroshi, please think about becoming maintainer for openssl. It
> will make everybody happy :-)

Becoming a maintainer fixes the 'closing ticket too soon' problem? I
don't think so. And I'm afraid but I'm already had enough projects
lined up. I think we should consider [ruby-dev:40741] for real (gem
out openssl for 1.9)

Regards,
// NaHi

=end

#14 - 03/29/2010 10:15 PM - mame (Yusuke Endoh)

=begin
Hi,

2010/3/29 NAKAMURA, Hiroshi nakahiro@gmail.com:

> On Sun, Mar 28, 2010 at 21:24, Yusuke ENDOH mame@tsg.ne.jp wrote:
>
> > However, such document investigation and major revamping take cost.
> > Because there is no maintainer for ruby-openssl, we can't help but
> > do superficial fix, unfortunately.
>
> The problem, for me, was closing the ticket without giving a time to
> identify the cost for fix.

Time will not solve a concern unless there is a person who
considers the concern, I think.

> Hiroshi, please think about becoming maintainer for openssl. ?It
> will make everybody happy :-)

Becoming a maintainer fixes the 'closing ticket too soon' problem?

I think so. If you are a maintainer, the ticket can be left
open with assigning to you. A release manager can ask you
the current status, and can encourage you to address/update
tickets assigned to you :-)

Okay, now I can verbalize more precisely what I really hate.
I hate open and NOT ASSIGNED tickets. They should be clarifed
where their responsibility lies. If there is no one who has
responsibility, it is unfortune but unavoidable to close
such tickets as WONTFIX.

--
Yusuke ENDOH mame@tsg.ne.jp

=end

#15 - 03/30/2010 10:26 AM - nahi (Hiroshi Nakamura)

=begin
Hi,

On Mon, Mar 29, 2010 at 22:15, Yusuke ENDOH mame@tsg.ne.jp wrote:

> The problem, for me, was closing the ticket without giving a time to
> identify the cost for fix.

Time will not solve a concern unless there is a person who
considers the concern, I think.

Even though I'd posted a question before closing? You don't allow
non-maintainer's contribution? I don't think you don't.

> Okay, now I can verbalize more precisely what I really hate.
> I hate open and NOT ASSIGNED tickets. They should be clarifed
> where their responsibility lies. If there is no one who has
> responsibility, it is unfortune but unavoidable to close
> such tickets as WONTFIX.

I prefer to keep those tickets untouched or label 'Information Needed'
status. Closing ticket too soon sometimes leads "Out of sight, out of
mind." It's good to let issue tracker express the project status as
it is.

Regards,
// NaHi

=end

#16 - 03/30/2010 07:09 PM - mame (Yusuke Endoh)

=begin
Hi,

2010/3/30 NAKAMURA, Hiroshi nakahiro@gmail.com:

> Okay, now I can verbalize more precisely what I really hate.
> I hate open and NOT ASSIGNED tickets. They should be clarifed
> where their responsibility lies. If there is no one who has
> responsibility, it is unfortune but unavoidable to close
> such tickets as WONTFIX.

I prefer to keep those tickets untouched or label 'Information Needed'
status. Closing ticket too soon sometimes leads "Out of sight, out of
mind." It's good to let issue tracker express the project status as

it is.

Agreed. I guess 'Feedback' exists for the status.

But I dislike it because 'Feedback' tickets appear in the list of 'open' tickets. It is cumbersome to grasp tickets that we must handle yet.

If there is a kind of label that means like 'Feedback' and does not appear in the list, such as 'Contribution Wanted', I'll use the label. But currently, there is no maintainer of redmine :-(

BTW, Christian Holtje, do you look the discussion? Could you please answer Hiroshi's question?

--
Yusuke ENDOH mame@tsg.ne.jp

=end

#17 - 05/14/2010 12:58 AM - docwhat (Christian Höltje)

=begin
Sorry for not responding sooner. I haven't been getting emails from redmine. I just switched my email address to gmail so we'll see if that fixes this problem.

I'm no expert with openssl, but you can see in code like this:
http://openssl.sourcearchive.com/documentation/0.9.8g/ex__data_8c-source.html

I went by the assumption that it needs to be NULL or a STACK. Looking at the code, I don't see it setting the STACK on initialization (GetX509Store), so I figured it should be NULL.

Ciao!
=end

#18 - 05/14/2010 01:08 AM - docwhat (Christian Höltje)

=begin
This was fixed in r27064.
=end

Files

openssl.patch	447 Bytes	03/24/2010	docwhat (Christian Höltje)