Ruby - Bug #12783

Segmentation fault when verifying RSA signature

09/22/2016 12:56 PM - toupeira (Markus Koller)

Status:	Closed		
Priority:	Normal		
Assignee:	rhenium (Kazuki Yamaguchi)		
Target version:			
ruby -v:	ruby 2.3.1p112 (2016-04-26 revision 54768) [x86_64-linux]	**Backport:**	2.1: UNKNOWN, 2.2: UNKNOWN, 2.3: UNKNOWN

Description

I ran into a segfault while using the json-jwt gem, it happens when trying to verify the RSA signature using the OpenSSL library. I've attached a minimal test case which triggers the segfault without going through json-jwt, along with the binary input data. The original non-binary format of the signature/JWT seems to be correct according to the validator at https://jwt.io/.

I'm on Debian sid with libssl 1.0.2h-1, and I could reproduce the segfault with several Ruby versions from 2.4.0-preview2 back to 2.1.10 (didn't try earlier ones). I also tried the newer libssl 1.1 (which caused compile errors with Ruby 2.3.1) as well as 1.0.1 (which I gave up on because I couldn't find out how to force Ruby to compile with the older version).

Let me know if there's more debugging information I can provide you with.

History

#1 - 09/23/2016 09:37 AM - rhenium (Kazuki Yamaguchi)

- Status changed from Open to Closed

- Assignee changed from MartinBosslet (Martin Bosslet) to rhenium (Kazuki Yamaguchi)

Thanks for reporting!

Fixed at upstream by commit:

https://github.com/ruby/openssl/commit/0e49794521db899ab25774e932f83d6ce452a8ec

Files

segfault.log	13.2 KB	09/22/2016	toupeira (Markus Koller)
segfault.rb	266 Bytes	09/22/2016	toupeira (Markus Koller)
signature	256 Bytes	09/22/2016	toupeira (Markus Koller)
signature_base_string	845 Bytes	09/22/2016	toupeira (Markus Koller)