Ruby master - Bug #9504

X509 certificate incorrectly loaded (because of try-pem-first-else-asn1)

02/08/2014 08:43 PM - rep (Mark Schloesser)

Status:	Feedback		
Priority:	Normal		
Assignee:	openssl		
Target version:			
ruby -v:	ruby 1.9.3p484 (2013-11-22 revision 43786) [x86_64-linux]	**Backport:**	

Description

Ruby's openssl extension tries to load certificates as PEM format first, and on failure will try to do DER / ASN1. The PEM format loading ignores junk in the beginning and end of the given buffer, which can lead to a DER certificate being incorrectly loaded. This occurs on 1.9.3 and 2.2.0.

More concretely this occurs in the wild when a server certificate has a X509 extension comment that includes another certificate in PEM format. Example below.

To fix this, one could allow the user to optionally specify the format, and do DER directly if specified. That would keep things backwards compatible and allow these certificates to be correctly parsed.

Example certificate - http://pastebin.com/V90dDSez
Openssl output for this - http://pastebin.com/GSsLtP8J

Ruby script to show the bug/problem - http://pastebin.com/Q7ap7FjN

I currently patched my ruby version (1.9.3) like this: http://pastebin.com/HzyyAm0p

Thanks for feedback and incorporating the patch / a similar solution for this into Ruby.

History

#1 - 02/08/2014 08:46 PM - rep (Mark Schloesser)

My patch means you can load the certificate like this:

```
x509 = OpenSSL::X509::Certificate.new(cert, "DER")
```

I guess having some module level constants for this (FILETYPE_PEM, FILETYPE_ASN1) would be better. Sadly I'm not a ruby guy by day, and I'd appreciate if someone cleans this up to be more clean :)

#2 - 03/03/2014 04:29 PM - nagachika (Tomoyuki Chikanaga)

- Status changed from Open to Assigned

- Assignee set to MartinBosslet (Martin Bosslet)

Hello, Mark.
Thank you for your reporting.

Martin, could you handle this?

#3 - 09/13/2015 03:10 AM - zzak (Zachary Scott)

- Assignee changed from MartinBosslet (Martin Bosslet) to openssl

#4 - 08/11/2019 05:41 PM - jeremyevans0 (Jeremy Evans)

- Backport deleted (1.9.3: UNKNOWN, 2.0.0: UNKNOWN, 2.1: UNKNOWN)

- Status changed from Assigned to Feedback

- File nested-asn1-9504.patch added

I worked on implementing support for adding a :format keyword to OpenSSL::X509::Certificate#initialize, allowing you to specify format: :der if you didn't want to try loading it as a PEM. A patch for that is attached (for the ruby-openssl repository).

For the certificate provided, using LibreSSL 3.0.0, both PEM_read_bio_X509 and d2i_X509_bio with the certificate return NULL, with the OpenSSL error: "nested asn1 error". Are you actually able to get the certificate to work with a modern version of OpenSSL or LibreSSL?

Files

nested-asn1-9504.patch	4.75 KB	08/11/2019	jeremyevans0 (Jeremy Evans)