Ruby master - Feature #9613

Warn about unsafe ossl ciphers

03/08/2014 03:04 AM - zzak (Zachary Scott)

Status:	Open
Priority:	Normal
Assignee:	openssl
Target version:	

Description

As of r45274, we now have sane whitelist of available OpenSSL ciphers. However, this patch breaks backwards compatibility for any apps that use any ciphers not whitelisted.

Solution

- Implement a new class: OpenSSL::SSL::Ciphers
  - This class defines a constant for every whitelisted cipher used by DEFAULT_PARAMS[:ciphers]
  - Any constant not found within this class should raise a warning and report to the user
- Add an OpenSSL::SSL::Configuration class
  - Designed to default to no compression, and no sslv2/v3
  - Used by DEFAULT_PARAMS[:options]
  - This class may contain helper methods such as: #compression_enabled?

Pros

- We don't break anything, without warning users first
- Maintaining future whitelist ciphers is easier
- Future unsupported/blacklist ciphers are already dismissed
- Users are able to extend cipher lists to support their needs (by adding a constant to OpenSSL::SSL::Ciphers)

Concerns

I have discussed this with Martin, and we'd like to open up this discussion for feedback. We're particularly concerned about backporting r45274 as it breaks compatibility. We should also consider:

- Do we backport both patches or just the warning?
- Should we bother backporting deprecation warnings?
  - Since r45274 is not a security fix, do we consider this a bug?
  - Rails only introduces deprecation notices in new minor releases (ie: Ruby-2.2.0)
- r45274 is a major change that could break existing apps, even considering security

Related issues:

Related to Backport21 - Backport #9640: Please backport SSL fixes to 2.1	**Closed**	**03/15/2014**

History

#1 - 03/17/2014 06:54 PM - naruse (Yui NARUSE)

- Related to Backport #9640: Please backport SSL fixes to 2.1 added

#2 - 03/18/2014 12:01 AM - zeha (Christian Hofstaedtler)

Single datapoint: r45274 will likely end up in Debian jessie's ruby 2.1, and by extension probably in Ubuntu's ruby 2.1.

#3 - 09/13/2015 03:27 AM - zzak (Zachary Scott)

- Tracker changed from Bug to Feature

- Assignee set to openssl