A TLS Renego coverage update

Yngve Nysæter Pettersen

Audun Mathias Øygard

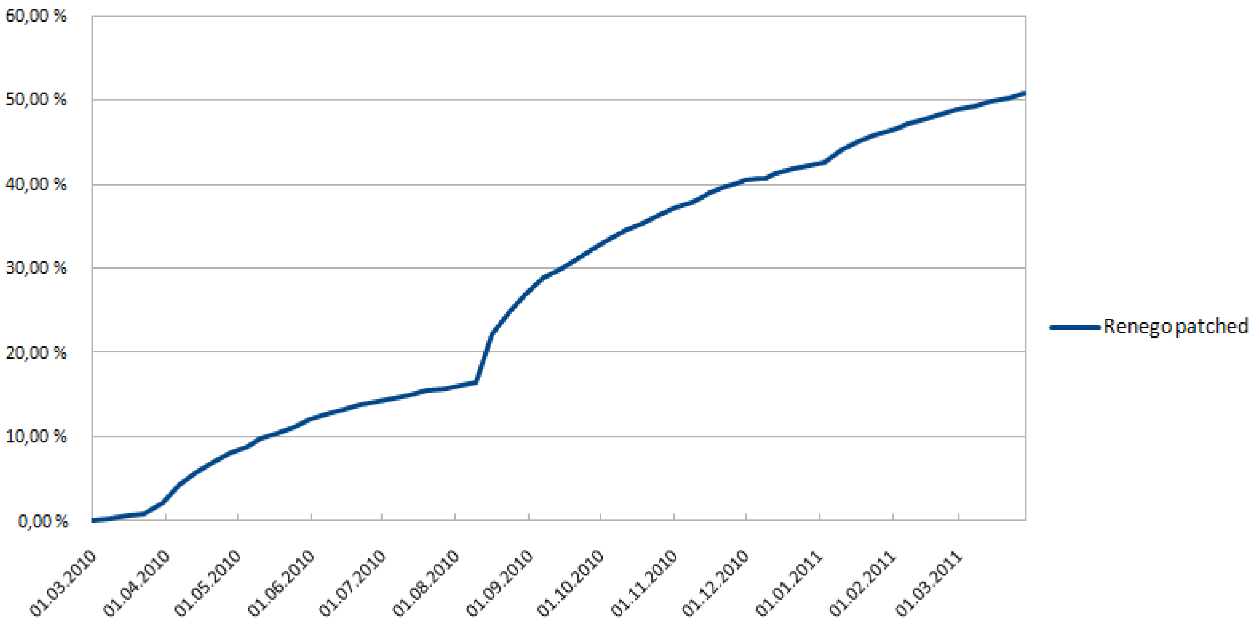
Opera Software ASA

http://my.opera.com/securitygroup/

IETF TLS WG meeting March 30, 2011

Renego status after 12 months

- Current coverage 50.8%
- 0.2% are not fully patched
- 70% are non-compliant in 4.x range
- Very few (<0.05%) are non-compliant up to TLS 1.2



Encryption

- 63% support SSL v2
- 48% (of total) support v2 exportable ciphers
- 1% support only SSL v3
- 63.5% support v3+ exportable ciphers
- 0.2% support only RC4/MD5

Extensions

- 7.9% support SNI
- 3% support Certificate Status
- Some (<50 known) Renego patched servers do not tolerate Renego+Certificate Status extension.

Top unpatched sites

- facebook.com
- yahoo.com + several TLD variations
- amazon.com
- wordpress.com
- ebay.com
- microsoft.com
- linkedin.com
- yandex.ru
- mail.ru
- vkontakte.ru
- flickr.com