Security Update:Are You Protected Against the FREAK Attack (and no, not the dance)?

Are You Protected Against the FREAK Attack (and no, not the dance)?

Status Type

Security Update

Private

Public

Date and Time

Wednesday, March 4, 2015 - 15:00

Reason

Security Vulnerability

Impact

SSL & TLS Users

WHAT HAPPENED?

A major security flaw has been discovered in the Secure Sockets Layer/Transport Layer Security (SSL/TLS) cryptographic protocols named the FREAK (Factoring RSA Export Keys) which affects many website and leaves many Apple and Google device users? exposed.

Advanced Users: For a complete description of the vulnerabilities and affected versions visit Tracking The Freak Attack at https://freakattack.com/ [1].

AFFECTED SOFTWARE and DEVICES:

- Open SSL
- Apple?s Safari Web Browser
- Google?s Android Phone?s Default Browser

- Other Software and embedded systems that run TLS

WHAT'S THE PROBLEM?

The weaker encryption key can be easily cracked and used to wage man-in-the-middle attacks on the secured connections in order to sniff passwords or other sensitive information.

WHAT DO I NEED TO DO?

1. Web Site Administrators

a. Check your site to determine if it is vulnerable:

1) On Linux and Unix (and possibly Mac OSX) you can run the following command: openssl s_client -connect hostname:443 -cipher EXPORT

- Substitute hostname with the FQDN of the server you?d like to test
- The correct response contains "handshake failure?. Any other response is a fail.

Note: A big thanks to Andrew Philipoff for providing this tip.

2) Run an automated SSL analyzer against the site; such as:

- https://www.ssllabs.com/ssltest/analyze.html; [2] or
- https://sslanalyzer.comodoca.com/ [3]

b. If the site you administer is vulnerable:

1) Open SSL = Upgrade to version 1.02 which was released in January 2015 - https://www.openssl.org/source/ [4].

2) Disable support for any export suites.

3) Instead of simply excluding RSA export cipher suites, disable support for all known insecure ciphers (e.g., there are export cipher suites protocols other than RSA) and enable forward secrecy.

2. General User

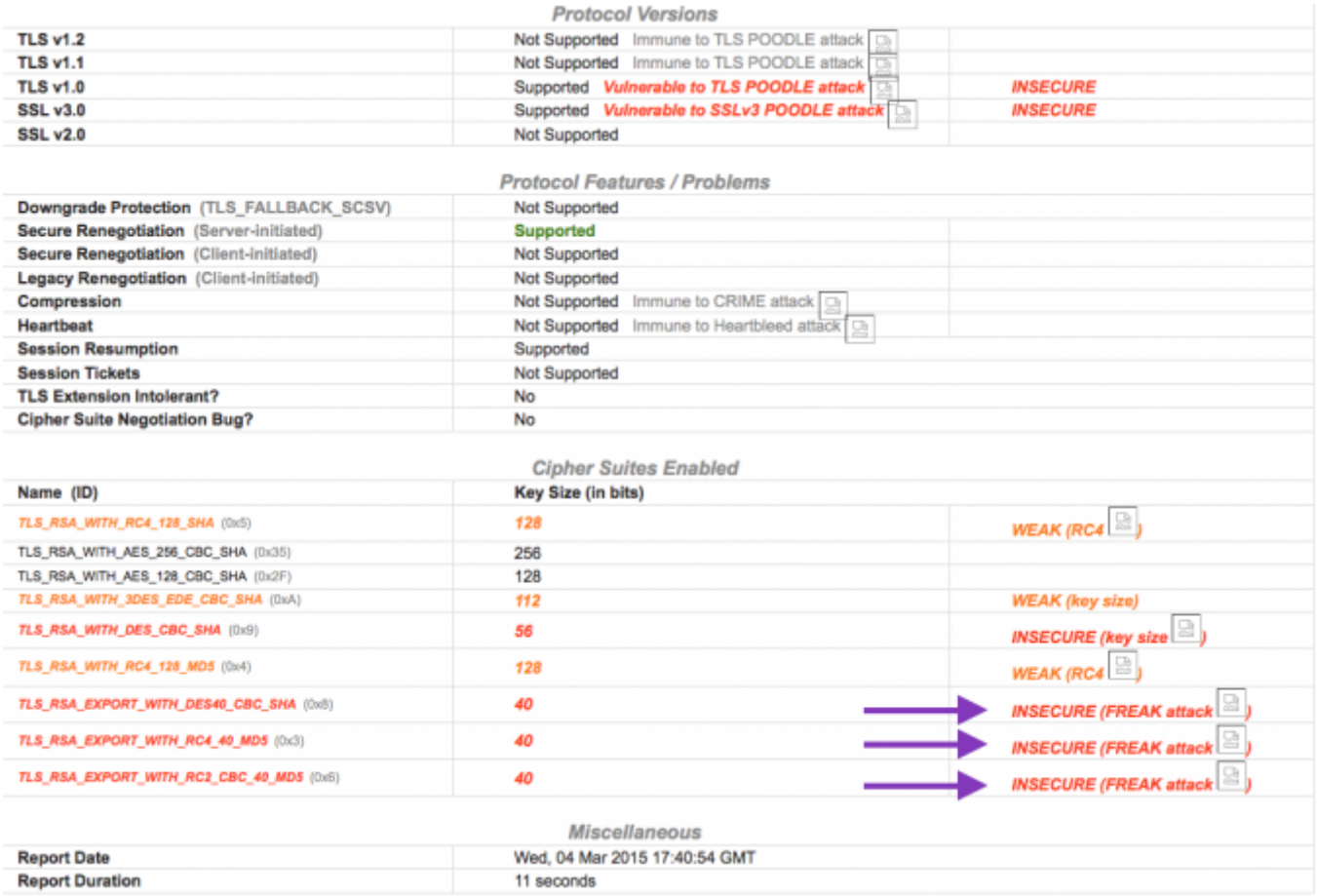
a. Check your browser to determine if it is vulnerable -https://freakattack.com/clienttest.html [5]

b. If vulnerable, update your software

- Apple and Google are preparing patches to be released in the near future.

c. Before visiting a website where you will be revealing sensitive information, you can check the security of the website by analyzing it through https://sslanalyzer.comodoca.com/ [3].

- At the bottom of the report it will list if the site is vulnerable:



Protocol Versions		
TLS v1.2	Not Supported Immune to TLS POODLE attack	
TLS v1.1	Not Supported Immune to TLS POODLE attack	
TLS v1.0	Supported *Vulnerable to TLS POODLE attack*	*INSECURE*
SSL v3.0	Supported *Vulnerable to SSLv3 POODLE attack*	*INSECURE*
SSL v2.0	Not Supported	

Protocol Features / Problems		
Downgrade Protection (TLS_FALLBACK_SCSV)	Not Supported	
Secure Renegotiation (Server-initiated)	Supported	
Secure Renegotiation (Client-initiated)	Not Supported	
Legacy Renegotiation (Client-initiated)	Not Supported	
Compression	Not Supported Immune to CRIME attack	
Heartbeat	Not Supported Immune to Heartbleed attack	
Session Resumption	Supported	
Session Tickets	Not Supported	
TLS Extension Intolerant?	No	
Cipher Suite Negotiation Bug?	No	

Cipher Suites Enabled		
Name (ID)	Key Size (in bits)	
TLS_RSA_WITH_RC4_128_SHA (0x5)	*128*	*WEAK (RC4)*
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256	
TLS_RSA_WITH_AES_128_CBC_SHA (0x2F)	128	
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xA)	*112*	*WEAK (key size)*
TLS_RSA_WITH_DES_CBC_SHA (0x9)	*56*	*INSECURE (key size)*
TLS_RSA_WITH_RC4_128_MD5 (0x4)	*128*	*WEAK (RC4)*
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8)	*40*	*INSECURE (FREAK attack)*
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3)	*40*	*INSECURE (FREAK attack)*
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6)	*40*	*INSECURE (FREAK attack)*

Miscellaneous	
Report Date	Wed, 04 Mar 2015 17:40:54 GMT
Report Duration	11 seconds

RELATED LINKS

- **Tracking The Freak Attack** - https://freakattack.com/ [1]
- **SMACK: State Machine AttaCKs** - https://www.smacktls.com/ [6]
- **ITS Security & Policy** - http://it.ucsf.edu/security [7]

Source URL: https://it.ucsf.edu/status/2015-03-04/are-you-protected-against-freak-attack-and-no-not-dance

Links
[1] https://freakattack.com/
[2] https://www.ssllabs.com/ssltest/analyze.html;

[3] https://sslanalyzer.comodoca.com/
[4] https://www.openssl.org/source/
[5] https://freakattack.com/clienttest.html
[6] https://www.smacktls.com/
[7] http://it.ucsf.edu/security