Google actualiza sus certificados SSL con claves de 2048 bits

Google anunció el jueves planes para reforzar el cifrado de las conexiones realizadas a sus servicios. La compañía tiene el objetivo de mejorar todos sus certificados SSL con claves de 2048 bits para finales de 2013.

Google también se cambia el certificado raíz que firma todos sus certificados SSL, ya que también se sigue utilizando una clave de 1024 bits menos seguro. La compañía dice que comenzará el cambio a los nuevos certificados de 2048 bits, el 1 de agosto, dándose un sólido cinco meses para «garantizar el tiempo necesario para una implementación cuidadosa antes de fin de año.»

Eso sigue siendo más de tres meses, pero Google está anunciando plan ahora porque sabe algunas configuraciones requieren medidas adicionales para evitar complicaciones. La compañía menciona específicamente el software de cliente integrado en dispositivos como algunos teléfonos, impresoras, set-decodificadores, consolas de juegos y cámaras.

Como resultado, el software de cliente que hace que las conexiones SSL a Google (por lo general en forma de HTTPS) debe adherirse a los siguientes requisitos:

- Realizar la validación normal de la cadena de certificados.
- Incluir una adecuada y amplia serie de certificados raíz que este contiene.
- Soporte a nombres alternativos del sujeto (SAN).

Para el segundo punto, Google ofrece un sistema de ejemplo en su FAQ que debería ser suficiente. Dicho esto, la empresa

avisa a los contenidos de la lista pueden cambiar con el tiempo, por lo que los clientes deben asegurarse de que tienen una forma de actualizar ellos mismos cuando se producen cambios.

Por último, pero no menos importante, Google indica que los clientes deberían, pero no están obligados a manejar el soporte de la extensión Server Name Indication (SNI), ya que puede ser necesario para realizar una llamada de una API adicional para establecer el nombre de host en una conexión SSL. Si no está seguro de que está utilizando SNI, puede probarlo contra https://googlemail.com – sólo este URL validará si envía SNI.