Google Encuentra Grave Vulnerabilidad En El Protocolo SSL

¿Te acuerdas de aquel seguro y confiable protocolo SSL? Resulta que este protocolo criptográfico, en el que hemos confiado para hacer más segura la comunicación a través de Internet tiene una grave vulnerabilidad en el protocolo de seguridad.

Los investigadores de Google anunciaron (enlace PDF) que han encontrado un **fallo en el protocolo SSL 3.0**. El exploit podría ser usado para **interceptar los datos sensibles** que se supone que son cifrados entre clientes y servidores.

El exploit permite a los atacantes iniciar un «downgrade» que le dice al cliente que el servidor no soporta el protocolo **TLS** (Transport Layer Security) y los obliga a conectarsen a través de la versión 3.0 de SSL. Desde allí, realizan un ataque man in the middle para descifrar las cookies seguras por HTTP. Google ha nombrado este ataque como ataque **POODLE** (Padding Oracle On Degradado Encryption Legacy).

En otras palabras, los datos ya no están encriptados y mucho menos protegidos. Los investigadores de Google Bodo Möller, el tailandés Duong y Krzysztof Kotowicz recomiendan deshabilitar la version 3.0 del protocolo SSL en los servidores y en los navegadores de los clientes, te contamos que ya hemos aplicado la recomendación en nuestros servidores ;) El servidor y el cliente con el **protocolo SSL** por defecto brindara mayor seguridad y la vulnerabilidad no será posible.

Para los usuarios finales, si su navegador soporta esta versión del protocolo, tienes que deshabilitar la version 3.0 de SSL 3.0, ó mejor aún, usar la herramienta que soporta TLS_FALLBACK_SCSV (Verificador de Transport Layer Security Suite), que previene los **ataques de downgrade**. Google dice que comenzará a realizar cambios para pruebas en Chrome que desactiva el uso de SSL 3.0. De hecho, ya existe un parche disponible para Chrome que deshabilita esta version del protocolo de seguridad.

En respuesta a esta noticia, Mozilla planea **desactivar SSL 3.0 en Firefox**. «SSLv3 será desactivado por defecto en Firefox 34, que será lanzado el próximo 25 de noviembre», anuncio Mozilla en un articulo. El código para desactivar el protocolo estará

disponible esta noche a través.

¿Cual Es La Utilidad De Este Protocolo De Seguridad?

El protocolo SSL fue introducido en 1996, este protocolo se supone que debe permitir la comunicación sin temor al espionaje, ya que la información que se comparte es encriptada. Cuando un cliente (navegador, aplicaciones, etc,) hace ping a un servidor, brinda una conexión bastante segura, la cual crea claves para cifrar y descifrar información enviada y recibida.