FREAK, El Fallo SSL Que Proviene De Los Estados Unidos

Siete horas es todo lo que se necesita para **romper el cifrado** que está en algunos sitios web, los cuales se suponen que son seguros. Los expertos en seguridad culpan a la prohibición del gobierno de Estados Unidos sobre el **uso de cifrado fuerte** en la década de 1990 para una vulnerabilidad que acaba de salir a la luz. Esta nueva vulnerabilidad ha sido llamada **FREAK** (Factoring attack on RSA-EXPORT Keys), existe la falla en los sitios web de alto perfil, incluyendo, irónicamente, la web de **NSA.gov**.

Las restricciones que limitan la seguridad en cifrados de 512 bits, se levantaron a finales de los años 90, pero no antes de que se desarrollara el software que está en uso hoy en día. La prohibición del envío de software con el cifrado fuerte parece hacer de las suyas, ya que encontró su camino de regreso a los Estados Unidos. Los **expertos en seguridad informática** dicen que el problema es grave, y la vulnerabilidad es relativamente fácil de explotar.

Matthew Green, un criptógrafo en el Instituto de Seguridad de la Información de Johns Hopkins, dijo que el gobierno de Estados Unidos había debilitado de manera efectiva su propia seguridad con la anterior prohibición a la exportación de cifrado fuerte.

La vulnerabilidad podría ser explotada en sitios vulnerables, con el cifrado débil en sólo siete horas. Es preocupante, si las muestras de prueba son correctos, más de una cuarta parte de los sitios web que se pensaba que son seguros, son vulnerables a este problema. En una entrada de blog, Green explica que la vulnerabilidad afecta el cifrado

de OpenSSL (utilizado por Android) y los clientes de Apple TLS / SSL (utilizado por Safari). Él continúa explicando que «el protocolo SSL en sí fue diseñado deliberadamente para ser roto» y que se podria lanzar un ataque de Man In The Middle en los sitios:

> *El cifrado de grado de exportación de 512 bits fue un compromiso entre tontos muy tontos. En teoría fue diseñado para asegurar que la NSA tendría la capacidad de acceder a las comunicaciones, mientras que supuestamente proporciona una encriptacion que todavía era «suficientemente buena» para el uso comercial. O si lo prefiere términos modernos, pensar en ella como la «llave maestra de oro» para los investigadores.*

En efecto, una puerta trasera puesta en marcha por el gobierno de Estados Unidos, ha dejado innumerables sitios web inseguros. Green resalta que la larga lista de sitios afectados incluye **connect.facebook.net** que se utiliza para usar el botón de Like de Facebook a millones de sitios web. Si esto fue secuestrado, las consecuencias podrían ser nefastas.