Vulnerabilidad En SSL/TLS Expone Datos En Texto Sin Formato

Vulnerabilidad En SSL/TLS Expone Datos En Texto Sin Formato

El esquema de cifrado más popular y ampliamente utilizado se ha encontrado vulnerable con la divulgación de un nuevo ataque que podría permitir a los atacantes **robar números de tarjetas de crédito**, contraseñas y otros datos sensibles de transmisiones protegidas por los protocolos SSL (Secure Sockets Layer) y TLS (Transport seguridad de la capa).

El ataque aprovecha una debilidad que lleva en funcionamiento 13 años, en el algoritmo de cifrado Rivest 4 (RC4), el cual cifra el flujo más utilizado para proteger el 30 por ciento del tráfico TLS en el Internet hoy.

Ataque BAR-MITZVAH

El ataque, denominado «**Bar-Mitzvah**«, puede llevarse a cabo incluso sin la realización de ataque man-in-the-middle (MITM) entre el cliente y el servidor, como en el caso de la mayoría de los hacks SSL anteriores.

Itsik Mantin, investigador de la empresa de seguridad Imperva, presentó los hallazgos en un estudio titulado, «**Atacar SSL cuando se utiliza RC4**» en la conferencia de seguridad Black Hat el jueves en Singapur.

E ataque Bar Mitzvah realmente explota la «Invariance

Weakness», los débiles modelo clave utilizado en llaves RC4 que pueden tener fugas de datos de texto sin formato encriptado por SSL / TLS en determinadas condiciones, exponiendo credenciales de cuenta, datos de tarjetas de crédito, u otra información sensible a los piratas informáticos.

La **Invariance Weakness** permite a un atacante distinguir flujos RC4 aleatorios y aumentar la probabilidad de fugas de datos sensibles en texto plano.

> *«La seguridad de RC4 [algoritmo] ha sido cuestionable desde hace muchos años, en particular, sus mecanismos de inicialización», escribieron los investigadores en un artículo de investigación (pdf).*
>
> *«Sin embargo, sólo en los últimos años ha comenzado a traducir este conocimiento en una llamada a retirarse RC4. En esta investigación, nosotros seguimos las investigaciones sobre [2013] RC4 y demostrar que el impacto de las vulnerabilidades conocidas en sistemas que utilizan RC4 está claramente subestimada.»*

Bar Mitzvah es el primer ataque «práctico» en SSL que sólo requiere inhalación pasiva o escuchas de conexiones cifradas con SSL / TLS. Aunque el investigador dice que un ataque MITM podría ser utilizado también para el secuestro de una sesión.

COMO PROTEGERSE

Los administradores deben considerar los siguientes pasos para protegerse de las debilidades RC4:

- Los administradores de **aplicaciones Web** deben desactivar RC4 en configuraciones TLS de sus aplicaciones.
- Los usuarios web deben desactivar RC4 en la configuración TLS de su navegador.
- Los proveedores de los navegadores debe considerar la

eliminación de RC4 de sus listas de cifrado TLS.

Durante los últimos años, varias vulnerabilidades significativas, incluyendo BEAST, POODLE, y el CRIME, han sido descubiertas en el protocolo SSL aprovechando la debilidad de RC4.