¿Por Qué Tienes Que Dejar De Usar WhatsApp?

El servicio de WhatsApp dirigido por el equipo de tan sólo 32 ingenieros, maneja más de 50 mil millones de mensajes diarios, y unos 385 millones de usuarios activos. La adquisición de WhatsApp por parte de Facebook, ha expuestos críticas sobre la seguridad de los miles de millones de mensajes entregados en la plataforma. Investigador de Seguridad en **Praetorian Labs** identificó varios **problemas de seguridad relacionados con SSL** en aplicación WhatsApp utilizando el **Project Neptune**, una plataforma de pruebas de **seguridad de aplicaciones móviles,** algo bastante interesante, ya que no importa si usas Whatsapp en español ó en otro idioma.

«La comunicación en WhatsApp entre tu teléfono y nuestro servidor está cifrada. Aunque los datos enviados por nuestra app están cifrados, acuerda que si tu dispositivo o el dispositivo de tu amigo está en uso por otra persona, es posible que esa persona podría leer tus mensajes WhatsApp. Debes ser consciente de la gente que tiene acceso a tu dispositivo.» Anuncio la compañía en su blog.

Pero los investigadores encontraron que WhatsApp es vulnerable a los ataques **Man-in-themiddle** porque la aplicación no ha solucionado problemas con el SSL, y por tanto, las credenciales de usuario pueden ser robadas fácilmente.

> *«WhatsApp no realiza el bloqueo de SSL cuando se establece una conexión de confianza entre las aplicaciones móviles y servicios web back-end. Sin SSL colocación de clavos forzada, un atacante podría man-in-the-middle la conexión entre las aplicaciones móviles y de back-end de servicios web . Esto permitiría al atacante para oler las credenciales de usuario, identificadores de sesión u otra información sensible «.*

WhatsApp está permitiendo que sus servidores en el back-end usen esquemas de cifrado de 40 bits y 56 bits, las cuales son débiles, estas pueden ser vulneradas usando ataque de fuerza bruta. 'Este es el tipo de cosas que la NSA le encantaría «, dijeron los investigadores.

El equipo de WhatsApp ha confirmado que están trabajando activamente en la **solución para el SSL** a su aplicación, pero aún eso no es suficiente para **proteger la privacidad**. Facebook y WhatsApp establecieron de que nada va a cambiar después de la adquisición y **WhatsApp** seguirá funcionando como un servicio independiente.

Las aplicaciones de mensajería móvil a menudo se usan para entregar los datos sensibles o para las comunicaciones personales y empresariales, por lo que los datos almacenados por el proveedor de servicios deben ser cifrados de extremo a extremo. Pero hay muchas otras aplicaciones de mensajería instantánea seguras y libres están disponibles como **Telegrama, SureSpot, Threema, TextSecure, RedPhone** etc, que usted debe utilizar para mantener su información privada y segura.