« La nueva tarjeta gráfica profesional de AMD mejora su rendimiento
Disponible Red Hat Enterprise Virtualization 3.4 »

Riesgos en el uso del WhatsApp

RedaccionMCP | 24/06/2014 |
1 comentario

WhatsApp ha alcanzado ya **los 500 millones de usuarios en todo el mundo** (en España su penetración es superior al 80%, lo que supone que más de 23 millones de personas se han descargado esta aplicación). Sus usuarios comparten **más de 50.000 millones de mensajes,** 700 millones de fotos y más de 100 millones de vídeos a diario, a lo que hay que sumar, desde agosto de 2013, los mensajes de voz.

El éxito de la aplicación, sin embargo, la ha situado e**n el punto de mira de los ciberatacantes** que, por qué no decirlo, se han encontrado en los diferentes ciclos de vida de la herramienta con una construcción **con las puertas abiertas de par en par.** Las numerosas vulnerabilidades encontradas la han situado como blanco perfecto para la distribución de malware y robo de datos personales. Esta situación se ha visto agravada por la escasa percepción de riesgos entre los usuarios de dispositivos móviles que apenas si toman precauciones para proteger su información (desde luego muchísimas menos que en otro tipo de dispositivos como los PC).

Las **críticas por la pésima gestión de la seguridad** se vieron incrementadas en febrero de este año tras anunciarse que Facebook compraba la compañía por 19.000 millones de dólares.

Principales vulnerabilidades

Pero, ¿cuáles son las principales vulnerabilidades en esta aplicación? Desde sus inicios se han ido descubriendo múltiples fallos de seguridad:

- **Falta de cifrado de sus comunicaciones** y, por tanto, el acceso a la agenda telefónica y a los mensajes de los usuarios conectados a Internet. Esta situación fue subsanada (eso sí, se ha comprobado que el cifrado es fácil de romper).

- Persisten las vulnerabilidades en la ubicación del usuario **a través del GPS,** puesto que WhatsApp almacena las coordenadas geográficas y las mantiene desprotegidas. De este modo, al compartir una ubicación (para lo cual la aplicación necesita la situación en Google Maps) los datos se descargan a través de un canal no seguro, sin utilizar SSL y sin cifrar.

- Juan Garrido, consultor de InnoTec System (del Grupo Entelgy) descubrió otra gran vulnerabilidad en marzo de 2013. Cualquier usuario, de forma anónima (sin necesidad de credenciales), **podía utilizar la infraestructura de WhatsApp para subir todo tipo de archivos o ficheros de cualquier tamaño a sus servidores** (incluido los ejecutables). Dado que, además, la plataforma de WhatsApp no cuenta con ningún tipo de antivirus y que los contenidos se borran automáticamente en un período de 30 días, las facilidades para distribuir todo tipo de malware o realizar ataques de phishing (haciendo creer al usuario que está ante la página web de su banco captando su contraseña) son tremendamente sencillas y sin ningún tipo de costes para el atacante (que además puede mantener el anonimato sin problema).

- Asimismo, Garrido descubrió **una grave carencia en el proceso de alta y verificación de los usuarios.** Así, el código de activación de usuario se genera en el propio entorno de la aplicación, incluso antes de ser enviado a los servidores internos para que éstos manden el mensaje SMS, con el código, al usuario.

Condiciones de uso y privacidad

Junto con las vulnerabilidades mencionadas, **hay otras cuestiones muy relevantes,** que van asociadas a las condiciones de uso de la propia aplicación y que no siempre son tenidas en cuenta por sus usuarios. Entre ellas se encuentran las siguientes:

- La compañía pueda acceder periódicamente a la lista de contactos y/o libreta de direcciones para mantener un registro de los números de teléfono de otros usuarios (es decir, no existe un consentimiento por parte de los contactos).
- Los datos denominados "Status Submission" (estados, fotos de perfil, información sobre si se está conectado o información sobre la última conexión) tienen una licencia no exclusiva, gratuita y transferible para usarlas, reproducirlas, distribuirlas, crear obras derivadas a partir de ellas, exhibirlas o comunicarlas.
- Sólo puede ser usado por mayores de 16 años (o menores con autorización paterna específica)
- Las condiciones pueden modificarse en cualquier momento, sin avisar. Es el usuario el responsable de revisarlas periódicamente.
- No garantiza la confidencialidad de conversaciones, ni de contenidos intercambiados.
- Los "Status Submission" no son borrados, se mantienen en las bases de datos de la compañía
- Está prohibido el uso comercial de la aplicación y la utilización de bots que envíen mensajes masivos.

Foto: Twin Design / Shutterstock.com