Miles de archivos GIF se comparte en WhatsApp a diario, en todo el mundo, pero lo que todas las personas no saben hasta ahora, es que por al menos tres meses estuvieron expuestas ataques cibernéticos por el simple hecho de compartir una imagen animada.

WhatsApp parchó recientemente una vulnerabilidad de seguridad crítica en su app para Android, que permaneció sin parches por al menos tres meses después de haber sido descubierta, y en caso de ser explotada, podría haber permitido que piratas informáticos remotos comprometan los dispositivos Android y potencialmente roben archivos y mensajes de chat.

La vulnerabilidad, rastreada como CVE-2019-11932, es un error de corrupción de memoria doblemente libre que en realidad no reside en el código de WhatsApp, sino en una biblioteca de análisis de imágenes GIF de código abierto que utiliza WhatsApp.

El fallo fue descubierto por el investigador de seguridad vietnamita, Pham Hong Nhat, en mayo de este año, y conduce con éxito a ataques de ejecución remota de código, lo que permite a los atacantes ejecutar código arbitrario en dispositivos específicos en el contexto de WhatsApp con los permisos que la aplicación tiene en el dispositivo.

> *«La carga útil se ejecuta en el contexto de WhatsApp. Por lo tanto, tiene el permiso para leer la tarjeta SD y acceder a la base de datos de mensajes de WhatsApp. El código malicioso tendrá todos los permisos que tiene WhatsApp, incluida la grabación de audio, el acceso a la cámara, el acceso al sistema de archivos, así como el almacenamiento sandbox de WhatsApp que incluye una base de datos de chat protegida, entre otros»*, dijo el investigador.

Funcionamiento de la vulnerabilidad RCE

WhatsApp utiliza la biblioteca de análisis en cuestión para generar una vista previa de los archivos GIF cuando los usuarios abren la galería de su dispositivo antes de enviar cualquier archivo multimedia.

Por lo tanto, se debe tener en cuenta que dicha vulnerabilidad no se activa al enviar un archivo GIF malicioso a una víctima, sino que se ejecuta cuando la propia víctima simplemente abre el Selector de Galería de WhatsApp mientras intenta enviar cualquier archivo multimedia a otra persona.

Para explotar la vulnerabilidad, todo lo que un hacker debe hacer es enviar un archivo GIF malicioso especialmente diseñada a un usuario Android objetivo por medio de cualquier canal de comunicación en línea y esperar a que el usuario simplemente abra la galería de imágenes de WhatsApp.

Sin embargo, si los atacantes desean enviar el archivo GIF a las víctimas a través de cualquier plataforma de mensajería como WhatsApp o Messenger, deben enviarlo como un archivo de documento en lugar de archivos adjuntos de medios, ya que la compresión de imágenes utilizada por estos servicios distorsiona la carga maliciosa oculta en las imágenes.

Como se muestra en el video de prueba de concepto que el investigador compartió con THN, la vulnerabilidad también se puede explotar para simplemente abrir un shell inverso de forma remota desde el dispositivo pirateado.

Este problema afecta a las versiones 2.19.230 de WhatsApp y versiones anteriores que se ejecutan en Android 8.1 y 9.0, pero no funciona para Android 8.0 y versiones posteriores.

> *«En las versiones anteriores de Android, el double-free todavía podía activarse. Sin embargo, debido a las llamadas malloc del sistema luego del double-free, la aplicación simplemente falla antes de llegar al punto en el que podríamos controlar el registro de la PC»*, dijo el investigador.

También mencionó que informó sobre la vulnerabilidad a Facebook, compañía propietaria de WhatsApp, a finales de julio, y que la compañía incluyó un parche de seguridad en WhatsApp versión 2.19.244, lanzado en septiembre.

Por lo tanto, es recomendable actualizar la versión de WhatsApp en Google Play Store lo antes posible. Además, debido a que la falla reside en una biblioteca de código abierto, también es posible que cualquier otra aplicación de Android que utilice la misma biblioteca afectada pueda ser vulnerable a ataques similares.

El desarrollador de la biblioteca GIF afectada, llamada Android GIF Drawable, también lanzó la versión 1.2.18 del software para parchear la vulnerabilidad double-free.