Una vulnerabilidad de alta gravedad, ahora parcheada en la función de filtro de imágenes de WhatsApp, podría haberse abusado para enviar una imagen maliciosa a través de la aplicación de mensajería para leer información confidencial de la memoria de la aplicación.

Rastreada como CVE-2020-1910, con puntuación CVSS de 7.8, la vulnerabilidad se refiere a una falla de lectura/escritura fuera de los límites y se deriva de la aplicación de filtros de imagen específicos a una imagen no autorizada y el envío de la imagen alterada a un destinatario involuntario, lo que permite a un atacante acceder a datos valiosos almacenados en la memoria de la aplicación.

> *«Una verificación de límites faltantes en WhatsApp para Android antes de la v2.21.1.13 y WhatsApp Business para Android antes de la v2.21.1.13 podría haber permitido la lectura y escritura fuera de los límites si un usuario aplicaba filtros de imagen específicos y envía la imagen resultante»,* dijo WhatsApp en febrero de 2021.

La compañía de seguridad cibernética Check Point Research, reveló el problema a la plataforma propiedad de Facebook el 10 de noviembre de 2020, dijo que pudo bloquear WhatsApp al cambiar entre filtros en los archivos GIF maliciosos.

Específicamente, el problema se originó en una función *«applyFilterIntoBuffer ()»*, que maneja los filtros de imagen, que toma la imagen de origen, aplica el filtro seleccionado por el usuario y copia el resultado en el búfer de destino.

Mediante la ingeniería inversa de la biblioteca *«libwhatsapp.so»*, los investigadores encontraron que la función vulnerable se basaba en la suposición de que tanto la fuente como las imágenes filtradas tienen las mismas dimensiones y también el mismo formato de color RGBA.

Debido a que cada píxel RGBA se almacena como 4 bytes, una imagen maliciosa que tenga solo 1 byte por píxel puede explotarse para lograr un acceso a la memoria fuera de los

límites, ya que la función *«intenta leer y copiar 4 veces la cantidad de la fuente asignada al búfer de imagen».*

WhatsApp dijo que *«no tiene motivos para creer que los usuarios se hayan visto afectados por este error»*. Desde la versión 1.21.1.13 de WhatsApp, la compañía ha agregado dos nuevas verificaciones en la imagen de origen y la imagen de filtro que aseguran que tanto las imágenes de origen como las de filtro estén en formato RGBA y que la imagen tenga 4 bytes por píxel para evitar lecturas no autorizadas.