WhatsApp parcheó de forma silenciosa el mes pasado, una vulnerabilidad crítica en su aplicación, que podría haber permitido a hackers comprometer de forma remota dispositivos específicos y potencialmente robar mensajes de chat seguros y archivos almacenados en ellos.

La vulnerabilidad, rastreada como CVE-2019-11931, es un problema de desbordamiento de búfer basado en la pila que residía en la forma en que las versiones anteriores de WhatsApp analizan los metadatos de flujo elemental de un archivo MP4, lo que resulta en ataques de denegación de servicio o ejecución remota de código.

Para explotar remotamente la vulnerabilidad, lo que necesita un atacante es el número de teléfono de los usuarios objetivo y enviarles un archivo MP4 creado de forma maliciosa por medio de WhatsApp, que eventualmente se puede programar para instalar una puerta trasera maliciosa o una aplicación de spyware en los dispositivos comprometidos en silencio.

La vulnerabilidad afecta a los consumidores y a las aplicaciones empresariales de WhatsApp para todas las plataformas principales, incluidas Android, iOS y Windows.

Según un aviso publicado por Facebook, la lista de versiones de app afectadas es la siguiente:

- Versiones de Android anteriores a 2.19.274
- Versiones de iOS anteriores a 2.19.100
- Enterprise Client versiones anteriores a 2.25.3
- Versiones de Windows Phone anteriores e incluidas 2.18.368
- Business para versiones de Android anteriores a 2.19.104
- Business para versiones de iOS anteriores a 2.19.100

El alcance y gravedad de la vulnerabilidad tuvo similitudes con una vulnerabilidad reciente de llamadas VoIP de WhatsApp, que fue explotada por la compañía israelí NSO Group para instalar el spyware Pegasus en casi 1400 dispositivos Android e iOS.

Hasta ahora, no está claro si la vulnerabilidad MP4 también fue explotada como un día cero en la naturaleza antes de que Facebook se haya entererado y la haya resparado.

Esta vulnerabilidad relacionada con archivos MP4, se da a solo dos semanas luego de que Facebook demandó a NSO Group por el mal uso del servicio de WhatsApp.

Mientras tanto, se recomienda a todos los usuarios que ejecuten la última versión de WhatsApp y deshabilitar las descargas automáticas de imágenes, archivos de audio y video.

Actualización: Un portavoz de WhatsApp confirmó a THN que la falla recientemente informada no fue explotada en la naturaleza.

> *«WhatsApp está trabajando constantemente para mejorar la seguridad de nuestro servicio. Hacemos informes públicos sobre los posibles problemas que hemos solucionado de forma coherente con las mejores prácticas de la industria. En este caso, no existe razón para creer que los usuarios se vieron afectados»,* dijo la compañía.