WhatsApp parchó recientemente un error de software muy frustrante, que podría haber permitido que un miembro de algún grupo bloquee la aplicación de los demás miembros.

Con el simple hecho de enviar un mensaje creado con fines malintencionados a un grupo, un atacante puede desencadenar un bloqueo de WhatsApp muy destructivo, obligando a todos los miembros del grupo a desinstalar completamente la aplicación, reinstalarla y eliminar el grupo para recuperar el funcionamiento normal.

Debido a que los miembros del grupo no pueden eliminar selectivamente el mensaje malicioso sin abrir la ventana del grupo y volver a activar el bucle de bloqueo, tienen que perder todo el historial de chat del grupo para deshacerse de él.

Descubierto por investigadores de la compañía israelí de seguridad cibernética, CheckPoint, el último error residió en la implementación del protocolo de comunicación XMPP de WhatsApp, que bloquea la aplicación cuando un miembro con un número de teléfono no válido envía un mensaje en el grupo.

> *«Cuando intentamos enviar un mensaje donde el parámetro 'participante' recibe un valor de 'nulo', se lanza una 'excepción de puntero nulo'»*, explicaron los investigadores.
>
> *«El analizador del número de teléfono del participante maneja mal la entrada cuando se recibe un número de teléfono ilegal. Cuando recibe un número de teléfono con una longitud, no en el guardabosques 5.20 o un carácter sin dígitos, lo leería como una 'cadena nula'»,* agregaron.

Este problema residía en WhatsApp para Android e iOS, pero en una entrevista con THN, el investigador de Check Point, Roman Zaikin, confirmó que el exploit funciona sin problemas contra todos los usuarios vulnerables de Android, pero a veces no se reproduce en iOS.

El ataque requiere que un miembro del grupo malintencionado manipule otros parámetros asociados con los mensajes en una conversación que de otro modo está protegida mediante cifrado de extremo a extremo.

Para llevar a cabo este ataque, un atacante puede aprovechar WhatsApp Web y una herramienta de depuración del navegador web en combinación con una herramienta de manipulación de código abierto WhatsApp que Check Point lanzó el año pasado.

La herramienta de manipulación de WhatsApp es una extensión para el software de prueba de penetración Burp Suite que permite a los usuarios interceptar, descifrar y volver a cifrar su comunicación de WhatsApp utilizando sus propias claves de cifrado.

Como se observa en el video, los investigadores utilizaron esta configuración para activar el error de bloqueo contra todos los miembros de un grupo simplemente reemplazando el parámetro del participante del número de teléfono del remitente a *'a@s.whatsapp.net'*, un dígito no válido de número de teléfono.

> *«El error bloqueará la aplicación, y seguirá bloqueándose incluso después de que volvamos a abrir WhatsApp, resultando en un ciclo de bloqueo. Además, el usuario no podrá volver al grupo y todos los datos que se escribieron y compartieron en el grupo ahora se han ido para siempre. El grupo no puede restaurarse después de que ocurra el bloqueo y tendrá que ser eliminado para detener el choque»,* dicen los investigadores.

Cabe mencionar que el ataque no afectaría al remitente, ya que el mensaje malicioso se inyectó en tránsito luego de salir del dispositivo del remitente.

Check Point informó responsablemente al equipo de seguridad de WhatsApp a fines de agosto de este año, y la compañía solucionó el problema con el lanzamiento de la versión 2.19.58 de WhatsApp a mediados de septiembre.

Los desarrolladores de WhatsApp también *«agregaron nuevos controles para evitar que las personas se agreguen a grupos no deseados para evitar la comunicación con partes que no son de confianza».*

> *«Debido a que WhatsApp es uno de los principales canales de comunicación del mundo para consumidores, empresas y agencias gubernamentales, la capacidad de detener a las personas que utilizan WhatsApp y eliminar información valiosa de los chats grupales, es un arma poderosa para los malos actores»,* dijo Oded Vanunu, jefe de producto de Check Point.