Facebook corrigió un error en su aplicación Messenger para Android, que pudo haber permitido a un hacker remoto llamar a objetivos desprevenidos y escucharlos incluso antes de que contesten la llamada de audio.

La vulnerabilidad fue descubierta y reportada a Facebook por Natalie Silvanovich, del equipo de búsqueda de errores de Project Zero de Google, el pasado 6 de octubre, e impacta la versión 284.0.0.16.119 o anteriores de Facebook Messenger para Android.

En otras palabras, la vulnerabilidad podría haber otorgado a un atacante que haya iniciado sesión en la aplicación, la opción de iniciar simultáneamente una llamada y enviar un mensaje especialmente diseñado a un objetivo que inició sesión tanto en la app como en otro cliente de Messenger, como el navegador web.

> *«Sería entonces desencadenar un escenario en el que, mientras que el dispositivo esté sonando, la persona que llama iniciaría la recepción de audio o bien, hasta que la persona que esté siendo llamada conteste»,* dijo Dan Gurfinkel, Gerente de Ingeniería de Seguridad de Facebook.

Según un informe técnico de Silvanovich, la falla reside en el Protocolo de Descripción de Sesión (SDP) de WebRTC, que define un formato estandarizado para el intercambio de medios de transmisión entre dos puntos finales, lo que permite a un atacante enviar un tipo especial de mensaje conocido como *«SdpUpdate»* que haría que la llamada se conectara al dispositivo de la persona que llama antes de ser respondida.

Las llamadas de audio y video a través de WebRTC generalmente no transmiten audio hasta que el destinatario haya hecho clic en el botón aceptar, pero si este mensaje «SdpUpdate» se envía al otro dispositivo mientras está sonando, *«hará que comience a transmitir audio de inmediato, lo que podría permitir a un atacante monitorear los alrededores de la persona que llama».*

De alguna forma, la vulnerabilidad tiene similitudes con una falla que erosiona la privacidad

que se informó en la función de chats grupales FaceTime de Apple el año pasado, que hizo posible que los usuarios iniciaran una videollamada FaceTime y escucharan a escondidas a los objetivos agregando su propio número como tercera persona en un chat grupal incluso antes de que la persona del otro lado aceptara la llamada entrante.

Pero a diferencia del error de FaceTime, explotar este problema no es tan sencillo. La persona que llama ya debería tener los permisos para llamar a una persona específica. En otras palabras, la persona que llama y la persona que recibe tendrían que se amigos de Facebook para lograr explotar la falla.

Además, el ataque requiere que el mal actor utilice herramientas de ingeniería inversa como *Frida*, para manipular su propia aplicación Messenger y obligarla a enviar el mensaje personalizado «SpdUpdate».

Silvanovich recibió una recompensa por errores de $60,000 dólares por informar sobre la vulnerabilidad, una de las tres recompensas por errores más altas de Facebook hasta ahora. El investigador de Google dijo que donaría a la organización sin fines de lucro GiveWell el total de su recompensa.

Silvanovich ha encontrado otras fallas críticas antes en las aplicaciones de mensajería como WhatsApp, iMessage, WeChat, Signal, Reliance.