Un equipo de investigadores académicos, que anteriormente descubrió graves problemas de seguridad en las redes 4G LTE y 5G, presentó hoy un nuevo ataque llamado *«ReVoLTE»*, que podría permitir a los atacantes remotos romper el cifrado utilizado por las llamadas de voz VoLTE y espiar llamadas telefónicas específicas.

El ataque no explota ninguna falla en el protocolo Voice Over LTE (VoLTE), pero aprovecha la implementación débil de la red móvil LTE por parte de la mayoría de los proveedores de telecomunicaciones, permitiendo al atacante espiar las llamadas telefónicas cifradas realizadas por las víctimas.

El protocolo VoLTE o Voice Over Long Term Evolution es una comunicación inalámbrica estándar de alta velocidad para teléfonos móviles y terminales de datos, incluidos los dispositivos y wearables de Internet de las Cosas (IoT), que implementan tecnología de acceso por radio 4G LTE.

El problema es que la mayoría de los operadores móviles por lo general utilizan el mismo flujo de claves para dos llamadas posteriores dentro de una conexión de radio para cifrar los datos de voz entre el teléfono y la misma estación base, es decir, la torre de telefonía móvil.

Por lo tanto, el nuevo ataque ReVoLTE aprovecha la reutilización del mismo flujo de claves por estaciones base vulnerables, lo que permite a los atacantes descifrar el contenido de las llamadas de voz impulsadas por VoLTE en el siguiente escenario.

Sin embargo, la reutilización de una secuencia de claves predecible no es nueva y fue señalada por primera vez por Raza & Lu, pero el ataque ReVoLTE lo convierte en un ataque práctico.

Funcionamiento de ReVoLTE

Para iniciar el ataque, el atacante debe estar conectado a la misma estación base que la

víctima y colocar un rastreador de enlace descendente para monitorear y grabar una *«llamada dirigida»* hecha por la víctima a otra persona, que necesita ser descifrada más tarde, como parte de la primera fase del ataque ReVoLTE.

Cuando la víctima cuelga la «llamada dirigida», se requiere que el atacante llame a la víctima, generalmente dentro de los 10 segundos posteriores, lo que obligaría a la red vulnerable a iniciar una nueva llamada entre la víctima y el atacante en la misma conexión de radio utilizada por la llamada dirigida anterior.

> *«La reutilización de la secuencia de claves se produce cuando el destino y la llamada de secuencia de claves utilizan la misma clave de cifrado de plano de usuario. Como esta clave se actualiza para cada nueva conexión de radio, el atacante debe asegurarse de que el primer paquete de la llamada de secuencia de claves llegue dentro de la fase activa»,* dijeron los investigadores.

Una vez conectado, como parte de la segunda fase, el atacante necesita involucrar a la víctima en una conversación y grabarla en texto plano, lo que ayudaría al atacante a calcular posteriormente el flujo de claves utilizado por la llamada posterior.

Según los investigadores, XOR-ing, los flujos de claves con el marco cifrado correspondiente de la llamada dirigida capturada en la primera fase descifra su contenido, lo que permite a los atacantes escuchar qué conversación tuvo su víctima en la llamada telefónica anterior.

> *«Como esto da como resultado el mismo flujo de claves, todos los datos RTP se cifran de la misma forma que los datos de voz de la llamada objetivo. Tan pronto como se generó una cantidad suficiente de datos del flujo de claves, el adversario cancela la llamada»,* dice la investigación.

Sin embargo, la duración de la segunda llamada debe ser mayor o igual que la primera para

descifrar cada trama, de lo contrario, solo se puede descifrar una parte de la conversación.

> *«Cabe señalar que el atacante tiene que involucrar a la víctima en una conversación más larga. Cuanto más tiempo ha hablado con la víctima, más contenido de la comunicación anterior puede descifrar»,* dicen los investigadores.
>
> *«Cada cuadro está asociado con un recuento y encriptado con un flujo de claves individual que extraemos durante el cálculo del flujo de claves. Como el mismo recuento genera el mismo flujo de claves, el recuento sincroniza los flujos de claves con los marcos cifrados de la llamada de destino. Los flujos de claves XOR-ing con la trama cifrada correspondiente descifra la llamada de destino».*
>
> *«Como nuestro objetivo es descifrar la llamada completa, la llamada de flijo de claves debe ser tan larga como la llamada de destino para proporcionar una cantidad suficiente de paquetes, ya que de lo contrario solo podemos descifrar una parte de la conversación».*

Detección y demostración de ReVoLTE

Para demostrar la viabilidad práctica del ataque ReVoLTE, el equipo de académicos de la Universidad de Ruhr en Bochum, implementó una versión de extremo a extremo del ataque dentro de una red comercial vulnerable y teléfonos comerciales.

El equipo utilizó el analizador de enlace descendente Airscope de Software Radio System, para rastrear el tráfico cifrado y tres teléfonos basados en Android para obtener el texto sin formato conocido en el teléfono del atacante. Luego comparó las dos conversaciones grabadas, determinó la clave de cifrado y finalmente descifró una parte de la llamada anterior.

Como se observa en el video, el ataque ReVoLTE podría costar menos de 7000 dólares a los atacantes para la configuración y descifrado del tráfico de enlace descendente.

El equipo probó una serie de célular de radio seleccionadas al azar en Alemania para determinar el alcance del problema y descubrió que afecta a 12 de las 15 estaciones base en Alemania, pero los investigadores dijeron que la brecha de seguridad también afecta a otros países.

Los investigadores notificaron a los operadores de estaciones base alemanas afectados sobre el ataque ReVoLTE, a través del proceso del Programa de Divulgación Coordinada de Vulnerabilidades de GSMA a inicios de diciembre de 2019, y los operadores lograron implementar los parches hasta ahora.

Debido a que el problema también afecta a una gran cantidad de proveedores en todo el mundo, los investigadores lanzaron una aplicación de Android de código abierto, llamada Mobile Sentinel, que puede usarse para detectar si la red 4G y estaciones base son vulnerables al ataque ReVoLTE.

Se puede ver más información en el sitio web dedicado y en el documento de investigación titulado «*Call Me Maybe: Eavesdropping Encrypted LTE Calls With REVOLTE*«.