Un grupo de investigadores de la Universidad de Ruhr Bochum y la Universidad de Nueva York, Abu Dhabi, descubrió fallas de seguridad en las redes 4G LTE y 5G que podrían permitir que los hackers se hagan pasar por usuarios en la red e incluso se registren para suscripciones de pago en nombre de otros.

El ataque de suplantación, denominado *«Ataques de IMPersonation en 4G NeTworks»* (IMP4GT), explota el método de autenticación mutua utilizado por el teléfono móvil y la estación base de la red para verificar sus respectivas identidades para la manipulación de los paquetes de datos en tránsito.

> *«Los ataques IMP4GT explotan la protección de integridad faltante para los datos del usuario y un mecanismo de reflexión del sistema operativo móvil de pila IP. Podemos utilizar el mecanismo de reflexión para construir un oráculo de cifrado y descifrado. Junto con la falta de protección de integridad, esto permite inyectar paquetes arbitrarios y descifrar paquetes»,* explicaron los investigadores.

Esta investigación fue presentada en el Simposio de Seguridad del Sistema Distribuido en Red (NDSS), el 25 de febrero de 2020, en San Diego, Estados Unidos.

Dicha vulnerabilidad afecta a todos los dispositivos que se comunican con LTE, incluyendo todos los smartphones, tabletas y dispositivos IoT que se venden actualmente.

> *«El equipo con sede en Bochum está intentando cerrar la brecha de seguridad en el último estándar de comunicación móvil 5G, que actualmente se implementa»*, agregaron los investigadores.

Las fallas fueron reveladas de forma responsable al organismo de estándares de telecomunicaciones GSM Association en mayo pasado.

Funcionamiento del ataque IMP4GT

Los investigadores llevaron a cabo los ataques utilizando radios definidas por software, que son dispositivos que pueden leer mensajes entre un teléfono y la estación base a la que está conectado. El ataque de hombre en el medio, permite que un hacker se haga pasar por un usuario hacia la red y viceversa.

El atacante entonces, engaña a la red para que crea que la radio era el teléfono (suplantación de enlace ascendente), y también engaña al teléfono para que asuma que la radio definida por software es la torre celular legítima (suplantación de enlace descendente).

> *«La suplantación del enlace ascendente permite que un atacante establezca una conexión IP arbitraria hacia Internet, por ejemplo, una conexión TCP a un servidor HTTP. Con la variante de enlace descendente, el atacante puede construir una conexión TCP al UE»,* dijeron los investigadores.

Cabe mencionar que el adversario debe estar muy cerca, en el rango de 2 km, del teléfono móvil de la víctima para poder montar el ataque IMP4GT. Como consecuencia, estos ataques no son diferentes de los que involucran simuladores de sitios celulares como los receptores de IMSI, que son utilizados por las agencias policiales para interceptar el tráfico de teléfonos móviles.

Una vez que el canal de comunicación se ve comprometido, la siguiente etapa del ataque funciona aprovechando la protección de integridad que falta en el estándar de comunicación LTE para modificar arbitrariamente los paquetes de datos que se intercambian.

Con el tráfico de Internet, el ataque podría permitir que un hacker realice compras no autorizadas, acceda a sitios web ilegales, cargue documentos confidenciales con la identidad de la víctima, o incluso, redirigir al usuario a un sitio malicioso, una forma diferente de

ataque llamada *«ataque posterior».*

> *«Este ataque tiene consecuencias de largo alcance para los proveedores y usuarios. Los proveedores ya no pueden suponer que una conexión IP se origina en el usuario. Los mecanismos de facturación pueden ser activados por un adversario, causando el agotamiento de los límites de datos, y cualquier control de acceso o firewall de los proveedores puede ser omitido»,* dijeron los investigadores.
>
> *«Al hacerlo, mostramos que un atacante puede pasar por alto el mecanismo de firewall del proveedor, y el teléfono está abierto a cualquier conexión entrante. Tal ataque es un trampolín para nuevos ataques, como la implementación de malware»,* agregaron.

La revelación del ataque IMP4GT se produce luego de una investigación parecida realizada por académicos de la Universidad de Purdue y la Universidad de Iowa, que descubrió tres nuevas fallas de seguridad en las redes 4G y 5G que pueden utilizarse para espiar llamadas telefónicas y rastrear las ubicaciones de los usuarios de teléfonos celulares.

El estándar 5G entrante, que se está implementando en varios países, tiene como objetivo ofrecer velocidades más rápidas y características de seguridad necesarias por mucho tiempo, incluida la protección contra los receptores MSI. Pero con cientos de millones afectados por estas fallas, es importante que las implementaciones de 5G apliquen una seguridad y protección de datos más robustas para corregir las vulnerabilidades.

> *«Los operadores de redes móviles tendrían que aceptar costos más altos, ya que la protección adicional genera más datos durante la transmisión. Además, todos los teléfonos móviles tendrían que ser reemplazados, y la estación base se expandiría. Eso es algo que no sucederá en el futuro cercano»,* dijo David Rupprecht, coautor de la investigación.