Vulnerabilidades recientemente descubiertas en el protocolo de comunicación moderno utilizado por los operadores de redes móviles (MNO), pueden explotarse para interceptar los datos del usuario y realizar ataques de suplantación, fraude y denegación de servicio (DoS).

Los hallazgos forman parte de un nuevo informe sobre vulnerabilidades en redes LTE y 5G de 2020, publicado por la compañía de seguridad cibernética Positive Technologies, con sede en Londres.

> *«Este documento abarca los resultados de las evaluaciones de seguridad realizadas durante el último período 2018-2019 en nombre de 28 operadores de telecomunicaciones en Europa, Asia, África y América del Sur».*

El Protocolo de Túnel GPRS (GTP), que es el estándar de comunicaciones basado en el Protocolo de Internet (IP) afectado, define un conjunto de reglas que rigen el tráfico de datos en redes 2G, 3G y 4G.

También forma la base de la red central GPRS y su sucesor Evolver Packet Core (EPC), lo que permite a los usuarios mantenerse conectados a Internet mientras se mueven de un lugar a otro.

> *«El protocolo GTP contiene una serie de vulnerabilidades que amenazan tanto a los operadores móviles como a sus clientes. Como resultado, los atacantes pueden interferir con el equipo de red y dejar una ciudad entera sin comunicaciones, hacerse pasar por usuarios para acceder a distintos recursos y usar servicios de red a expensas del operador o suscriptores»*, dijo la compañía.

La falla principal se debe al hecho de que el protocolo no verifica la ubicación real del suscriptor, lo que dificulta la verificación del tráfico válido entrante.

Otro problema arquitectónico reside en la forma en que se verifican las credenciales del suscriptor, lo que permite que los malos actores falsifiquen el nodo que actúa como SGSN (Serving GPRS Support Node).

En un escenario alternativo, un actor malicioso puede secuestrar datos de sesión de usuario que contienen identificadores relevantes de un suscriptor real para hacerse pasar por esa persona y acceder a Internet.

> *«Estos ataques también pueden ser utilizados por un MNO deshonesto para crear tráfico de itinerancia, con el MNO cobrando falsamente a otro operador por la actividad de itinerancia inexistente de los suscriptores de ese operador»,* dice el informe.
>
> *«En todas las redes probadas, era posible usar Internet móvil a expensas de los otros suscriptores y del operador».*

Con las redes 5G haciendo uso de EPC como la red central para las comunicaciones inalámbricas, Positive Technologies dijo que son igualmente vulnerables a la falsificación y los ataques de divulgación.

Agregó que cada red probada era susceptible a la denegación de servicio contra equipos de red, evitando así que los suscriptores válidos se conecten a Internet y da como resultado la interrupción de los servicios de comunicación móvil.

> *«La pérdida masiva de comunicación es especialmente peligrosa para redes 5G, ya que sus suscriptores son dispositivos IoT como equipos industriales, hogares inteligentes e infraestructura de la ciudad»,* dijeron los investigadores.

Para mitigar los problemas de seguridad, la empresa instó a los operadores a llevar a cabo un filtrado de IP basado en la lista blanca a nivel GTP, además de seguir las recomendaciones de seguridad de GSMA para analizar el tráfico en tiempo real, así como tomar medidas para bloquear la actividad ilegítima.

> *«La seguridad debe ser una prioridad durante el diseño de la red. Esto es más cierto ahora que nunca, ya que los operadores comienzan a abordar la construcción de redes 5G. Los intentos de implementar la seguridad como una ocurrencia tardía en las etapas posteriores pueden costar mucho más: es probable que los operadores necesiten comprar equipos adicionales, en el mejor de los casos. En el peor de los casos, los operadores pueden estar atrapados con vulnerabilidades de seguridad a largo plazo que no se pueden solucionar más adelante»,* concluye el informe.