Conforme las redes se implementan gradualmente en las principales ciudades del mundo, un análisis de su arquitectura de red ha revelado una serie de posibles debilidades que podrían explotarse para llevar a cabo una serie de ataques cibernéticos, incluidos los de denegación de servicio (DoS) para privar a los suscriptores del acceso a Internet e interceptar el tráfico de datos.

Los hallazgos forma la base de una nueva «Investigación de Seguridad Central 5G Independiente«, publicada ayer por la compañía de seguridad cibernética con sede en Londres, Positive Technologies, exactamente seis meses después de que la compañía publicara su informe *«Vulnerabilidades en LTE y redes 5G 2020»* en junio, que detalla fallas de alto impacto en protocolos LTE y 5G.

> *«Los elementos clave de la seguridad de la red incluyen la configuración adecuada de los equipos, así como la autenticación y autorización de los elementos de la red»*, dijo Positive Technologies.

«En ausencia de estos elementos, la red se vuelve vulnerable a la denegación de servicio del suscriptor debido a la explotación de vulnerabilidades en el protocolo PFCP», y otras deficiencias que podrían conducir a la divulgación de identificadores únicos de suscriptor e información de perfil, e incluso al uso de servicios de Internet a cargo del usuario sin su conocimiento.

Uno de los beneficios de seguridad clave que ofrece 5G es la protección contra la vigilancia de mantarrayas y el cifrado de números de identidad de suscriptor móvil internacional (IMSI), identificadores únicos que vienen con cada tarjeta SIM con el propósito de identificar a los usuarios de una red celular.

El 5G Core (5GC) también actualiza la pila de protocolos de TI utilizando el Protocolo de Control de Transmisión (TCP) como protocolo de capa de transporte en lugar del Protocolo de Transmisión de Control de Flujo (SCTP), HTTP/2 como sustituto del protocolo Diameter para la seguridad de la capa de aplicación y una capa TLS adicional para la comunicación encriptada

entre todas las funciones de la red.

Implementada en modo autónomo o no autónomo dependiendo de su dependencia de la tecnología 4G Envolver Packet Core (EPC), la red móvil 5G es un marco que consta de hasta nueve funciones de red (NF) que son responsables de registrar suscriptores, administrar sesiones y perfiles de abonado, almacenando datos de abonado y conectando a los usuarios (UE o equipo de usuario) a Internet a través de una estación base (gNB).

Pero los investigadores afirman que esta misma pila de tecnologías potencialmente abre la puerta a ataques a los suscriptores y la red del operador que podrían explotarse para organizar ataques de intermediario y DoS.

Ataques DoS y MitM

Un aspecto problemático de la arquitectura del sistema es la interfaz dedicada a la gestión de sesiones (función de gestión de sesiones o SMF) a través de un protocolo llamado Protocolo de Control de Reenvío de Paquetes (PFCP).

Un mal actor puede optar por enviar un paquete PFCP de solicitud de modificación o eliminación de sesión, provocando una condición de DoS que, a su vez, conduce a la interrupción del acceso a Internet (puntuación CVSS 6.1) e incluso a la interceptación del tráfico web (puntuación CVSS 8.3).

Positive Technologies también encontró problemas con la parte del estándar 5G que gobiernan la función de repositorio de red (NRF), que permite el registro y descubrimiento de NF en el plano de control, y señaló que los adversarios podrían agregar una función de red ya existente en el repositorio para atender a los suscriptores a través de una NF bajo su control y acceder a los datos del usuario.

En un escenario diferente, se podría abusar de la falta de autorización en NRF para cancelar el registro de componentes críticos al eliminar sus perfiles NF correspondientes de la tienda, lo que resultaría en la pérdida de servicio para los suscriptores.

Además, se destaca un par de vulnerabilidades de autenticación de suscriptores que pueden aprovecharse para revelar el Identificador Permanente de Suscripción (SUPI) asignado a cada suscriptor y servir al usuario final utilizando la información de autenticación filtrada mediante la suplantación de una estación base.

Por otro lado, una peculiaridad de diseño en el módulo User Data Management (UDM) que administra los datos del perfil del suscriptor podría permitir que un adversario con *«acceso a la interfaz relevante se conecte al UDM directamente o haciéndose pasar por un servicio de red, y luego extraiga toda la información necesaria»*, incluidos los datos de ubicación (puntuación CVSS de 7.4).

> *«El acceso a tales datos pondría en grave peligro la seguridad: permite al atacante espiar en secreto al suscriptor, mientras que este último nunca sabrá qué está pasando»,* dijeron los investigadores.

Finalmente, un atacante puede hacerse pasar por el módulo de la función de administración de acceso y movilidad (AMF) que se encarga del registro del suscriptor en la red mediante el uso de la información de identificación del suscriptor para crear nuevas sesiones de Internet sigilosas por las que se facturará al suscriptor.

> *«Los operadores frecuentemente cometen errores en la configuración de los equipos con consecuencias para la seguridad. Los proveedores de equipos desempeñan un papel importante, que son responsables de la implementación técnica de todas las funciones de protección de red diseñadas»,* dijeron los investigadores.

> *«Para prevenir las consecuencias de tales ataques, los operadores deben emplear medidas de protección oportunas, como la configuración adecuada del equipo, el uso de firewalls en el borde de la red y el monitoreo de la seguridad»,* agregaron.