Una investigación nueva sobre la arquitectura 5G descubrió una falla de seguridad en sus funciones de red virtualizadas y de corte de red que podrían explotarse para permitir el acceso a datos y ataques de denegación de servicio entre diferentes cortes de red 5G de un operador móvil.

AdaptiveMobile compartió sus hallazgos con la Asociación GSM (GSMA) el 4 de febrero de 2021, después de eso, las vulnerabilidades fueron designadas colectivamente como CVD-2021-0047.

5G es una evolución de la tecnología actual de red celular de banda ancha 4G, se basa en lo que se llama arquitectura basada en servicios (SBA), que proporciona un marco modular para implementar un conjunto de funciones de red interconectadas, lo que permite a los consumidores descubrir y autorizar su acceso un conjunto de servicios.

Las funciones de red también son responsables de registrar suscripciones, administrar sesiones y perfiles de suscripciones, almacenar datos de suscriptores y conectar a los usuarios (UE o equipo de usuario) a Internet a través de una estación base (gNB). Además, cada función de red de la SBA puede ofrecer un servicio específico pero al mismo tiempo también puede solicitar un servicio de otra función de red.

Una de las formas en que se organiza el núcleo de la SBA de la red 5G es a través de un modelo de segmentación. La idea del modelo es «cortar» la arquitectura de red original en múltiples redes virtuales lógicas e independientes que están configuradas para cumplir con un propósito comercial específico, que a su vez, dicta los requisitos de calidad de servicio (QoS) necesarios para eso.

Además, cada segmento de la red central consta de un grupo lógico de funciones de red (NF) que pueden asignarse exclusivamente a ese segmento o compartirse entre distintos segmentos.

Dicho de otro modo, al crear segmento separados que priorizan ciertas características, permite a un operador de red crear soluciones personalizadas para industrias particulares.

Por ejemplo, se puede utilizar un segmento de banda ancha móvil para facilitar el entretenimiento y los servicios relacionados con Internet, un segmento de Internet de las Cosas (IoT) se puede usar para ofrecer servicios adaptados a los sectores minorista y de fabricación, mientras que se puede designar un segmento de baja latencia independiente para necesidades de misión crítica como la salud y la infraestructura.

> *«El 5G SBA ofrece muchas características de seguridad que incluyen lecciones aprendidas de generaciones anteriores de tecnologías de red. Pero por otro lado, 5G SBA es un concepto de red completamente nuevo que abre la red a nuevos socios y servicios. Todos estos conducen a nuevos desafíos de seguridad»,* dijo AdaptiveMobile en un análisis de seguridad.

Según la compañía de seguridad de redes móviles, esta arquitectura no solo plantea nuevas preocupaciones de seguridad que surgen de la necesidad de admitir funciones heredadas, sino también de un *«aumento masivo en la complejidad del protocolo»* como consecuencia de la migración de 4G a 5G, y en el proceso abriendo la puerta a una multitud de ataques, como:

- Acceso malicioso a un segmento mediante la fuerza bruta de su diferenciados de segmento, un valor opcional establecido por el operador de red para distinguir entre segmentos del mismo tipo, lo que permite que un segmento no autorizado obtenga información no autorizada de un segundo segmento, como la función de gestión de acceso y movilidad (AMF), que mantiene el conocimiento de la ubicación de un equipo de usuario.
- Denegación de servicio (DoS) contra otra función de red aprovechando un segmento comprometido.

Los ataques dependen de una peculiaridad de diseño de que no hay comprobaciones para

garantizar que la identidad del segmento en la solicitud de la capa de señalización coincida con la utilizada en la capa de transporte, lo que permite que un adversario conectado al SBA del operador 5G a través de una función de red no autorizada se apodere de la red central, además de los segmentos de red.

Cabe mencionar que la capa de señalización es la capa de aplicación específica de telecomunicaciones que se utiliza para intercambiar mensajes de señalización entre funciones de red que se encuentran en diferentes segmentos.

Como contramedidas, AdaptiveMobile recomienda dividir la red en distintas zonas de seguridad aplicando filtros de seguridad de señalización entre diferentes segmentos, la red central y socios externos, y las funciones de red compartidas y no compartidas, además de implementar una solución de protección de capa de señalización para salvaguardar contra ataques de fuga de datos que aprovechan la correlación faltante entre capas.

Aunque la arquitectura 5G actual no admite un nodo de protección de este tipo, el estudio sugiere mejorar el proxy de comunicación de servicio (SCP) para validar la exactitud de los formatos de mensajes, hacer coincidir la información entre capas y protocolos y proporcionar funcionalidad relacionada con la carga para evitar ataques DoS.

> *«Este tipo de enfoque de filtrado y validación permite la división de la red en zonas de seguridad y la protección de la red central 5G. La correlación cruzada de la información de los ataques entre esas funciones de la red de seguridad maximiza la protección contra atacantes sofisticados y permite mejores mitigaciones y una detección más rápida al tiempo que minimiza las falsas alarmas»,* dijeron los investigadores.