Google ha desvelado las nuevas medidas de seguridad implementadas en sus dispositivos Pixel más recientes para enfrentar la creciente amenaza de los ataques a la seguridad del *baseband*.

El *baseband* celular, que se refiere al módem, es un procesador en el dispositivo que gestiona toda la conectividad, incluyendo LTE, 4G y 5G, con una torre de telefonía móvil o estación base a través de una interfaz de radio.

«Esta función implica inherentemente el procesamiento de entradas externas, que pueden provenir de fuentes no confiables», explicaron Sherk Chung y Stephan Chen del equipo de Pixel, junto con Roger Piqueras Jover e Iván Lozano del equipo de Android, en una publicación de blog.

> *«Por ejemplo, actores maliciosos pueden usar estaciones base falsas para inyectar paquetes de red falsificados o manipulados. En protocolos como IMS (IP Multimedia Subsystem), esto puede hacerse de forma remota desde cualquier lugar del mundo utilizando un cliente IMS».*

Además, el firmware que gestiona el *baseband* celular puede tener vulnerabilidades que, si se explotan correctamente, podrían comprometer la seguridad del dispositivo, particularmente en situaciones que permitan la ejecución remota de código.

En una presentación de Black Hat USA en agosto pasado, un equipo de ingenieros de seguridad de Google calificó al módem como un componente «esencial» y «crítico» en los teléfonos inteligentes, con acceso a datos sensibles y que puede ser accedido de forma remota a través de varias tecnologías de radio.

Las amenazas al *baseband* no son meramente teóricas. En octubre de 2023, una investigación de Amnistía Internacional reveló que la alianza Intellexa, detrás del software espía *Predator*, desarrolló una herramienta llamada Triton para explotar vulnerabilidades en el software *baseband* Exynos usado en dispositivos Samsung, permitiendo el despliegue de

este spyware en ataques altamente dirigidos.

El ataque se lleva a cabo mediante una degradación forzada, que obliga al dispositivo objetivo a conectarse a la red 2G mediante un simulador de estación base. Luego, se utiliza un transceptor de estación base 2G (BTS) para distribuir el software malicioso.

Google ha lanzado una nueva característica de seguridad en Android 14 que permite a los administradores de TI deshabilitar la compatibilidad con redes 2G en los dispositivos administrados. También destacó el uso de sanitizadores de Clang (IntSan y BoundSan) para fortalecer la seguridad del *baseband* celular en Android.

A principios de este año, la compañía también reveló que está trabajando con socios del ecosistema para implementar nuevas alertas que notifiquen a los usuarios de Android si su conexión de red no está cifrada o si una estación base falsa o herramienta de vigilancia está rastreando su ubicación utilizando un identificador de dispositivo.

La empresa también ha detallado las medidas que está adoptando para combatir el uso de simuladores de estaciones base, como los Stingrays, por parte de actores maliciosos, que inyectan mensajes SMS directamente en los teléfonos Android, un método conocido como fraude *SMS Blaster*.

> *«Este método de inyección de mensajes evita completamente la red del operador, eludiendo así todos los sofisticados filtros de anti-spam y anti-fraude basados en la red. Los SMS Blasters exponen una red LTE o 5G falsa, cuya única función es degradar la conexión del usuario a un protocolo 2G obsoleto»,* señaló Google en agosto.

Entre las otras defensas que Google ha integrado en su nueva línea de Pixel 9 están los *stack canaries*, la integridad del flujo de control (CFI) y la auto-inicialización de las variables de la pila a cero, para evitar la filtración de datos sensibles o ser utilizados para la ejecución de código.

> *«Los stack canaries funcionan como dispositivos de seguridad que garantizan que el código se ejecute en el orden esperado. Si un atacante intenta explotar una vulnerabilidad en la pila para alterar el flujo de ejecución sin tener en cuenta el canary, el canary 'se activa', alertando al sistema de un posible ataque»,* explicó Google.

> *«De manera similar, la CFI asegura que la ejecución del código solo ocurra a lo largo de un conjunto limitado de rutas. Si un atacante trata de desviarse de esas rutas permitidas, la CFI provoca que el módem se reinicie en lugar de seguir un camino no autorizado».*