Google está alertando sobre un conjunto de vulnerabilidades de seguridad graves en los chips Exynos de Samsung, algunas de las cuales podrían explotarse de forma remota para comprometer completamente un teléfono sin requerir la interacción del usuario.

Las 18 vulnerabilidades de día cero afectan a una amplia gama de smartphones Android de Samsung, Vivo, Google, dispositivos portátiles que utilizan el conjunto de chips Exynos W920 y vehículos equipados con el conjunto de chips Exynos Auto T5123.

Cuatro de las 18 vulnerabilidades hacen posible que un hacker logre acceder a Internet en Samsung, Vivo y Google, así como dispositivos portátiles que utilizan el chipset Exynos W920 y vehículos de fines de 2022 y principios de 2023.

> *«Las cuatro vulnerabilidades permiten a un atacante comprometer remotamente un teléfono a nivel de banda base sin interacción del usuario, y solo requieren que el atacante sepa el número de teléfono de la víctima»,* dijo Tim Willis, jefe de Google Project Zero.

Al hacerlo, un atacante podría obtener acceso arraigado a la información celular que entra y sale del dispositivo objetivo. Se omitieron detalles adicionales sobre las vulnerabilidades.

La ejecución de los ataques puede parecer prohibitiva, pero por el contrario, están al alcance los hackers expertos, que pueden diseñar rápidamente un exploit operativo para violar los dispositivos afectados *«de forma silenciosa y remota».*

Se cree que las 14 vulnerabilidades restantes no son tan graves, ya que requieren un infiltrado interno en la red móvil o un atacante con acceso local al dispositivo.

Aunque los teléfonos Pixel 6 y 7 ya recibieron una solución como parte de las actualizaciones de seguridad de marzo de 2023, se espera que los parches para otros dispositivos varíen según el cronograma del fabricante.

Hasta entonces, se recomienda a los usuarios qu apaguen las llamdas WiFi y Voice over LTE (VoLTE) en la configuración de su dispositivo para *«eliminar el riesgo de explotación de las vulnerabilidades».*