Google resolvió un problema de seguridad de alta gravedad que afecta a todos los teléfonos inteligentes Pixel, y que podría explotarse trivialmente para desbloquear los dispositivos.

La vulnerabilidad, rastreada como CVE-2022-20465 e informada por el investigador de seguridad David Schütz en junio de 2022, se remedió como parte de la actualización mensual de Android de Google para noviembre de 2022.

> *«El problema permitió que un atacante con acceso físico eludiera las protecciones de la pantalla de bloqueo (huella digital, PIN, etc.) y obtuviera acceso completo al dispositivo del usuario»*, dijo Schütz, quien recibió $70,000 dólares por descubrir la omisión de la pantalla de bloqueo.

El problema, según el investigador, radica en el hecho de que las protecciones de la pantalla de bloqueo se anulan por completo al seguir una secuencia específica de pasos:

- Proporcionar la huella dactilar incorrecta tres veces para deshabilitar la autenticación biométrica en el dispositivo bloqueado
- Intercambiar en caliente la tarjeta SIM en el dispositivo con una SIM controlada por un atacante que tenga un código PIN configurado
- Ingresar el pin SIM incorrecto tres veces cuando se solicita, bloqueando la tarjeta SIM
- El dispositivo solicita al usuario que ingrese el código de clave de desbloqueo personal (PUK) de la SIM, un número único de 8 dígitos para desbloquear la SIM
- Ingresar un nuevo código PIN para la SIM controlada por el atacante
- El dispositivo se desbloquea de forma automática

Esto también significa que todo lo que un atacante necesita para desbloquear un teléfono Pixel es traer su propia tarjeta SIM bloqueada con PIN y estar en posesión del código PUK de la tarjeta.

> *«El atacante podría simplemente cambiar la SIM en el dispositivo de la víctima y realizar el exploit con una tarjeta SIM que tuviera un bloqueo de PIN y para la cual el atacante sepa el código PUK correcto»,* dijo Schütz.

Un análisis de las confirmaciones del código fuente realizado por Google para reparar la falla muestra que es causado por un *«estado incorrecto del sistema»* introducido como resultado de una interpretación incorrecta del evento de cambio de SIM, lo que hace que se descarte completamente la pantalla de bloqueo.

«No se esperaba causar un cambio de código tan grande en Android con este error», agregó Schütz.