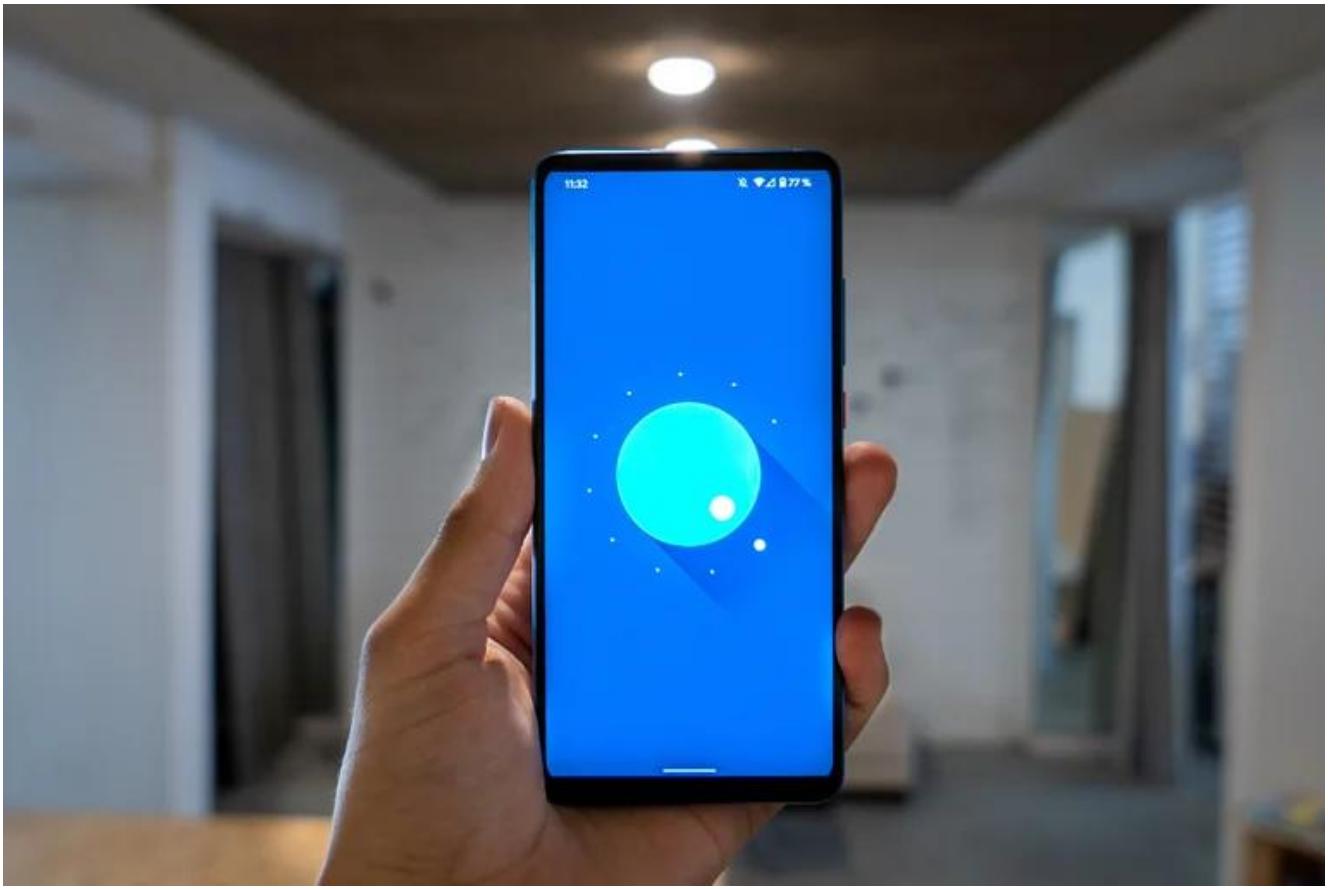
Celulares Android deben actualizarse: cibercriminales encontraron la forma de acceder al celular sin la clave

19/11/2022



Cruzar la pantalla de bloqueo de un teléfono requiere introducir un pin, patrón o reconcomiendo facial, sin embargo, un investigador en ciberseguridad encontró una vulnerabilidad con la que los delincuentes podrían aprovechar para acceder al celular sin tener la clave.

David Schütz fue el experto que encontró el fallo en los dispositivos **Android**, por lo que llamó la atención de **Google**, quienes ya corrigieron el fallo con un parche para los

dispositivos con este sistema, por lo que la recomendación es verificar y actualizar el teléfono constantemente.

Cómo era el proceso de ingreso

Todo arranca reiniciando el celular, ya que este debe pedir el pin de seguridad para entrar el teléfono. Lo que hizo **Schütz** fue ingresar tres veces mal el código y eso generó que la SIM se bloqueara, por lo que ingresó el PUK (la clave de desbloqueo personal) para restaurarla.

Pero cuando el móvil volvió a arrancar no le pidió la contraseña, sino que pusiera su huella para el desbloqueo, algo que no debe suceder en ningún dispositivo, porque eso es una opción que se da una vez se haya puesto el pin al encenderlo.

De esta forma, si un delincuente inserta su propia SIM en el celular de la víctima, luego ingresa el PIN incorrectamente tres veces, puede ingresar el PUK de su SIM y crear un nuevo pin para tener acceso total al dispositivo.

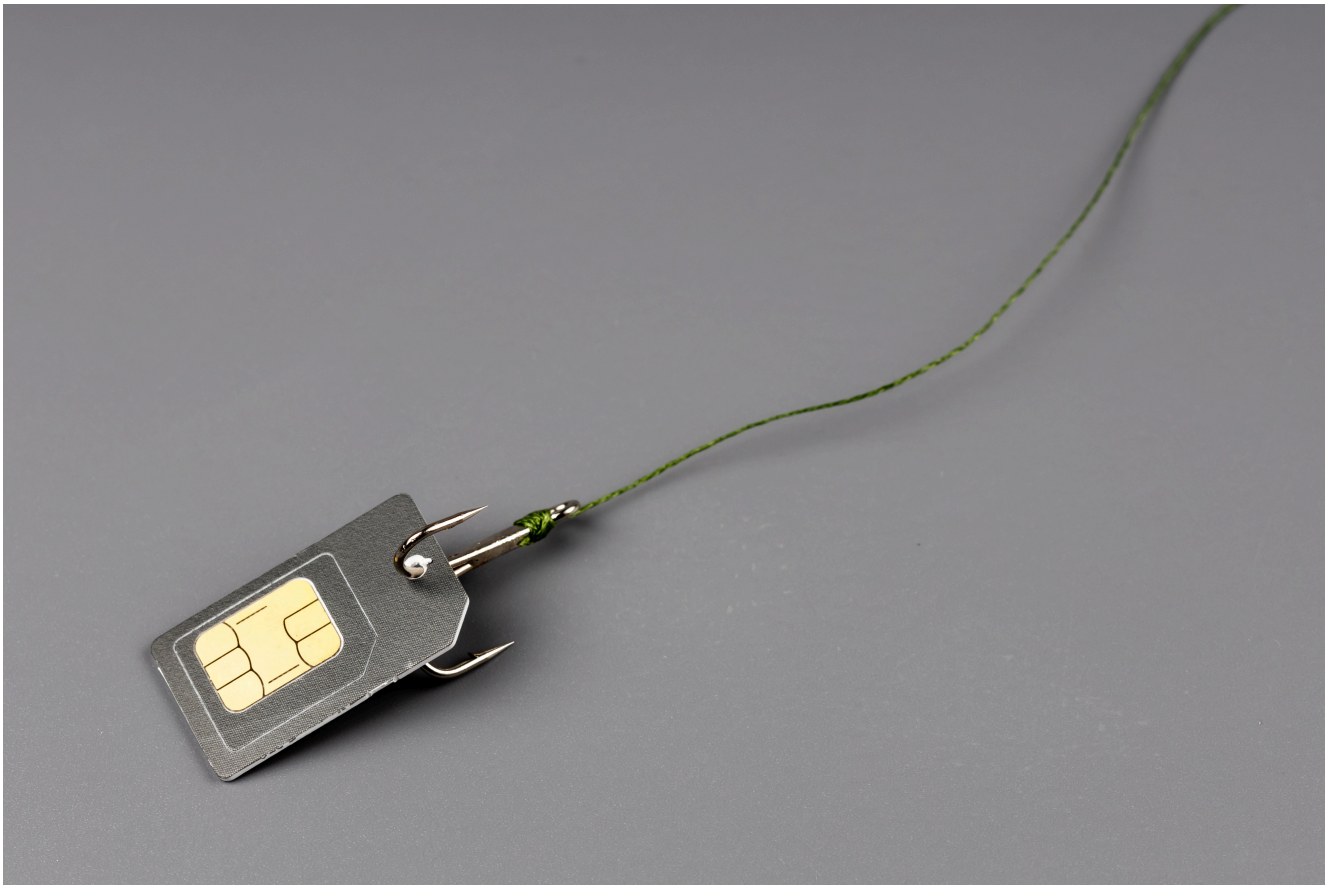
Ya con esa vulnerabilidad el delincuente puede modificar otras configuraciones se seguridad, información personal, correo y ver todo el contenido al tener la posibilidad de usar el móvil como si fuera suyo.

Solución a este fallo

Google ya corrigió la situación con un parche, por lo que los usuarios que tengan Android 10, 11, 12 y 13 deben descargar la actualización de seguridad de noviembre de 2022 para evitar esta vulnerabilidad.

Para hacerlo se debe ir a Configuración> Sistema > Actualización de sistema, luego buscar una nueva actualización, descargarla e instalarla. Otro método para obtener el parche es yendo a Configuración> Seguridad>

Comprobación de seguridad de **Google**, desde ahí también se puede hacer el proceso para tener el teléfono a salvo.



Un investigador encontró un fallo de seguridad en teléfonos al modificarle la SIM y cambiar el PIN de la pantalla de bloqueo.

Te puede interesar:

Software espía

El **Grupo de Análisis de Amenazas de Google** (TAG) dio a conocer que identificó un software espía en dispositivos móviles de **Samsung**, que llegó a explorar vulnerabilidades en los dispositivos, aunque la situación ya fue controlada y corregida.

Fueron tres vulnerabilidades las que se usaron como una cadena para tomar parte del control del celular, ya que los atacantes tenían privilegios para leer y modificar archivos para luego exponerlos.

Según la investigación los celulares en los que se realizaron los ataques eran los que utilizaban el kernel 4.14.113 y el procesador **Exynos,** que se comercializa principalmente en Europa, Medio Oriente y África.

Además, las referencias en las que fue identificado el espionaje fueron el Galaxy S10, A50 y A51, donde se llevaba a los usuarios a descargar un archivo por fuera de las tiendas oficiales, que le permitió al ciberdelincuente huir de la zona de pruebas de la aplicación diseñada para contener su actividad y acceder al resto del sistema operativo del dispositivo.

Esta situación ya fue corregida por **Samsung,** que se comprometió a divulgar las vulnerabilidades que se explotan activamente, como ya lo están haciendo **Google y Apple.**

Fuente: Infobae