Se han revelado múltiples vulnerabilidades críticas en las aplicaciones de Android preinstaladas de Samsung, que de ser explotadas exitosamente, podrían haber permitido a los atacantes acceder a datos personales sin el consentimiento de los usuarios y tomar el control de los dispositivos.

> *«El impacto de estas vulnerabilidades podría haber permitido a un atacante acceder y editar los contactos, SMS/MMS de la víctima, instalar aplicaciones arbitrarias con derechos de administrador del dispositivo o leer y escribir archivos arbitrarios en nombre de un usuario del sistema que podrían cambiar la configuración del dispositivo»,* dijo Sergey Toshin, fundador de la compañía de seguridad móvil, Oversecured.

Toshin informó sobre las vulnerabilidades a Samsung en febrero de 2021, después de lo cual, el fabricante emitió parches como parte de sus actualizaciones de seguridad mensuales para abril y mayo. La lista de las 7 vulnerabilidades es la siguiente:

- CVE-2021-25356: Omisión de autenticación de terceros en el aprovisionamiento administrado
- CVE-2021-25388: Vulnerabilidad de instalación arbitraria de aplicaciones en Knox Core
- CVE-2021-25390: Redirección de intención en PhotoTable
- CVE-2021-25391: Redirección de intenciones en carpeta segura
- CVE-2021-25392: Es posible acceder al archivo de política de notificación de DeX
- CVE-2021-25393: Posibilidad de acceso de lectura/escritura a archivos arbitrarios como usuario del sistema (afecta a la aplicación Configuración)
- CVE-2021-25397: Escritura arbitraria de archivos en TelephonyUI

El impacto de estas vulnerabilidades significa que podrían explotarse para instalar aplicaciones arbitrarias de terceros, otorgar privilegios de administrador al dispositivo para eliminar otras aplicaciones instaladas o robar archivos confidenciales, leer o escribir archivos arbitrarios como usuario del sistema e incluso ejecutar acciones privilegiadas.

En una demostración de prueba de concepto (PoC), Oversecured estableció que era posible aprovechar las vulnerabilidades de redirección de intenciones en PhotoTable y Secure Folder para secuestrar los permisos de las aplicaciones para acceder a la tarjeta SD y leer los contactos almacenados en el teléfono. Del mismo modo, al explotar CVE-2021-25397 y CVE-2021-25392, un atacante podría sobrescribir el archivo que almacena mensajes SMS/MMS con contenido malicioso y robar datos de las notificaciones de los usuarios.

Se recomienda a los usuarios de dispositivos Samsung que apliquen las últimas actualizaciones de firmware de la empresa para evitar riesgos de seguridad.