Una investigación reveló una serie de vulnerabilidades graves en Find My Mobile, una aplicación de Android que viene preinstalada en la mayoría de los smartphones Samsung. Las vulnerabilidades podrían haber permitido a hackers remotos rastrear la ubicación de las víctimas en tiempo real, monitorear llamadas telefónicas, mensajes e incluso eliminar datos almacenados en el teléfono.

El proveedor de servicios de seguridad cibernética con sede en Portugal, Char 49, reveló sus hallazgos sobre la aplicación de Android, Find My Mobile, de Samsung, en la conferencia DEF CON la semana pasada.

> *«Esta falla, después de la configuración, puede explotarse fácilmente y con graves implicaciones para el usuario, con un impacto potencialmente catastrófico: denegación permanente del servicio mediante el bloqueo del teléfono, pérdida completa de datos con restablecimiento de fábrica (tarjeta SD incluida), implicación grave de privacidad a través de IMEI y rastreo de ubicación, así como acceso al registro de llamadas y SMS»*, dijo Pedro Umbelino, de Char49.

Las vulnerabilidades, que funcionan en dispositivos Samsung Galaxy S7, S8 y S9+ sin parches, fueron abordadas por Samsung luego de marcar el exploit como *«una vulnerabilidad de alto impacto».*

El servicio Find My Mobile de Samsung permite a los propietarios de dispositivos localizar o bloquear de forma remota su teléfono inteligente o tableta, hacer una copia de seguridad de los datos almacenados en los dispositivos en Samsung Cloud, borrar los datos locales y bloquear el acceso a Samsung Pay.

Según Char49, había cuatro vulnerabilidades diferentes en la aplicación que pudieron haber sido explotadas por una aplicación maliciosa instalada en el dispositivo objetivo, creando de este modo un ataque de hombre en el disco para secuestrar la comunicación de los servidores backend y espiar a la víctima.

La falla se debe al hecho de que la aplicación verifica la presencia de un archivo específico en la tarjeta SD del dispositivo («/mnt/sdcard/fmm.prop») para cargar una URL («mg.URL»), lo que permite una aplicación maliciosa para crear este archivo que puede ser utilizado por un mal actor para potencialmente secuestrar las comunicaciones con el servidor.

> *«Al apuntar la URL de MG a un servidor controlado por un atacante y forzar el registro, el atacante puede obtener muchos detalles sobre el usuario: ubicación aproximada a través de la dirección IP, IMEI, marca del dispositivo, nivel de API, aplicaciones de respaldo y otra información»*, dijo Umbelino.

Para lograr esto, una aplicación maliciosa instalada en el dispositivo hace uso de una cadena de exploits que aprovecha dos receptores de transmisión desprotegidos diferentes para redirigir los comandos enviados a los servidores de Samsung desde la aplicación Find My Mobile a un servidor diferente que está bajo el control del atacante y ejecutar comandos maliciosos.

El servidor malicioso también reenvía la solicitud al servidor legítimo y recupera la respuesta, pero no sin antes inyectar sus propios comandos en las respuestas del servidor.

Al hacerlo, un ataque exitoso podría permitir a un hacker rastrear la ubicación del dispositivo, obtener datos de llamadas y mensajes de texto para espiar, bloquear el teléfono para obtener un rescate y borrar todos los datos mediante un restablecimiento de fábrica.

> *«La aplicación FMM no debería tener componentes arbitrarios disponibles públicamente y en un estado exportado. Si es absolutamente necesario, por ejemplo, si otros paquetes llaman a estos componentes, entonces deben protegerse con los permisos adecuados. Se debe eliminar el código de prueba que se basa en la existencia de archivos en lugares públicos»,* dijo Umbelino.