Varias aplicaciones muy utilizadas en la tienda Google Play Store para dispositivos Android están expuestas a una vulnerabilidad relacionada con la manipulación de rutas, lo que podría permitir que una aplicación maliciosa sobrescriba archivos arbitrarios en el directorio principal de la aplicación vulnerable.

Según un informe publicado el miércoles por el equipo de Inteligencia de Amenazas de Microsoft, las consecuencias de esta vulnerabilidad podrían incluir la ejecución de código no autorizado y el robo de tokens, dependiendo de cómo esté implementada cada aplicación.

Si la vulnerabilidad es explotada con éxito, un atacante podría obtener el control total del comportamiento de la aplicación afectada y utilizar los tokens robados para acceder de forma no autorizada a las cuentas en línea y otros datos sensibles del usuario.

Entre las aplicaciones identificadas como vulnerables se encuentran:

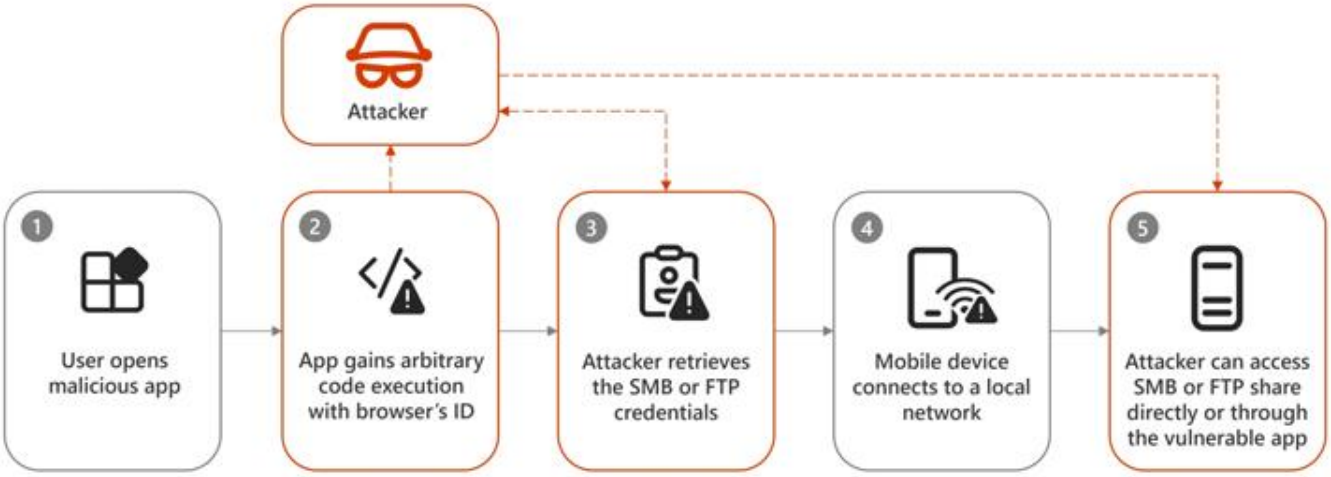
- Xiaomi File Manager (com.mi.Android.globalFileexplorer) – Con más de 1 mil millones de instalaciones
- WPS Office (cn.wps.moffice_eng) – Con más de 500 millones de instalaciones

Aunque Android está diseñado para aislar cada aplicación en su propio espacio de datos y memoria, utiliza un *«proveedor de contenido»* para permitir que las aplicaciones compartan datos y archivos de manera segura. Sin embargo, algunos errores en la implementación podrían permitir que una aplicación eluda las restricciones de lectura y escritura en su directorio principal.

Según explicó Valsamaras, este modelo de *«proveedor de contenido»* debería facilitar un intercambio seguro de archivos entre aplicaciones. No obstante, es común encontrarse con situaciones en las que la aplicación que recibe el archivo no valida su contenido y, lo que es más preocupante, utiliza el nombre de archivo proporcionado por la aplicación que lo envía para almacenarlo en su directorio de datos interno.

Este error podría tener consecuencias graves si la aplicación que envía el archivo utiliza una

versión maliciosa de la clase FileProvider para compartir archivos entre aplicaciones, lo que podría llevar a que la aplicación receptora sobrescriba archivos críticos en su propio espacio de datos.



En resumen, este mecanismo se aprovecha de la confianza ciega de la aplicación receptora en los datos recibidos, permitiendo que se envíen cargas arbitrarias con un nombre de archivo específico mediante un intento personalizado y explícito, sin el consentimiento del usuario, lo que puede conducir a la ejecución de código malicioso.

Como resultado, un atacante podría sobrescribir el archivo de preferencias compartidas de la aplicación objetivo y establecer una comunicación con un servidor bajo su control para extraer información sensible.

Otro escenario posible implica aplicaciones que cargan bibliotecas nativas desde su propio directorio de datos en lugar de la ubicación estándar, lo que podría permitir que una aplicación maliciosa sobrescriba una biblioteca nativa con código malicioso.

Tras una divulgación responsable, tanto Xiaomi como WPS Office han corregido este problema desde febrero de 2024. Sin embargo, Microsoft advierte que esta vulnerabilidad

podría ser más común de lo que se cree y urge a los desarrolladores a revisar sus aplicaciones en busca de problemas similares.

Google también ha emitido pautas para los desarrolladores, instándoles a manipular correctamente los nombres de archivo proporcionados por las aplicaciones servidoras.

> *«Cuando la aplicación cliente guarde el archivo recibido, debe ignorar el nombre de archivo proporcionado por la aplicación servidora y usar un identificador único generado internamente. Si no es posible generar un nombre de archivo único, la aplicación cliente debería limpiar el nombre de archivo proporcionado»*, explicó Google.