Informe De Pruebas De Vulnerabilidad

Integrantes: Mauricio Veliz Y Bayron Perez.

Aplicación: GPSMapApp

Fecha del Análisis: 25 de octubre de 2024

Herramientas: MobSF (Mobile Security Framework).

Índice

1. Resumen Ejecutivo

Este informe documenta las pruebas de seguridad realizadas en la aplicación GPSMapApp para identificar y mitigar posibles vulnerabilidades. Se llevaron a cabo pruebas de análisis estático y dinámico que revelaron varias vulnerabilidades críticas que afectan tanto la seguridad como la privacidad de los usuarios. Este documento describe cada vulnerabilidad encontrada, las pruebas realizadas, el impacto potencial y las recomendaciones para mitigarlas.

2. Metodología de Pruebas

Las pruebas de vulnerabilidad se realizaron en dos fases principales:

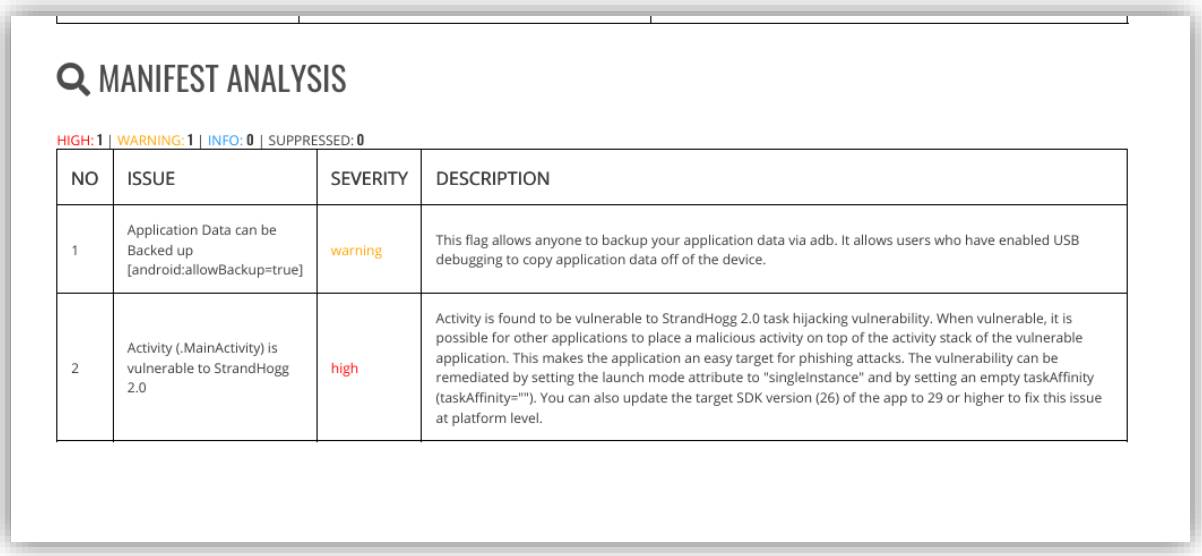
- **Análisis Estático:** Se utilizó MobSF para escanear el código fuente y la configuración de la aplicación, identificando vulnerabilidades en los permisos, configuraciones de manifiesto, y el uso de protocolos de red.
- **Análisis Dinámico:** Se simularon escenarios de uso real en un emulador, monitoreando el comportamiento de la aplicación en cuanto al uso de permisos, tráfico de red, y exposición de datos.

3. Resultados del Análisis Estático

Vulnerabilidad	Descripción	Impacto	Recomendación
Permitir Respaldo de Datos	android:allowBackup en true permite que los datos de la aplicación sean respaldados sin control.	Exposición de datos sensibles	Cambiar allowBackup a false.
Vulnerabilidad de StrandHogg 2.0	.MainActivity permite la superposición de actividades, lo que facilita ataques de phishing mediante secuestro de tareas.	Ataques de phishing	Configurar launchMode y taskAffinity.
Conexiones No Seguras (HTTP)	La aplicación realiza conexiones mediante HTTP, lo que expone los datos a interceptaciones.	Riesgo de interceptación de datos	Usar solo HTTPS para tráfico de red.

3.1 Capturas de Pantalla:

Captura de análisis a android:allowBackup del archivo AndroidManifest.xml. y Extracto del análisis de MobSF mostrando la vulnerabilidad de StrandHogg 2.0.



MANIFEST ANALYSIS

HIGH: 1 | WARNING: 1 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
2	Activity (.MainActivity) is vulnerable to StrandHogg 2.0	high	Activity is found to be vulnerable to StrandHogg 2.0 task hijacking vulnerability. When vulnerable, it is possible for other applications to place a malicious activity on top of the activity stack of the vulnerable application. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" and by setting an empty taskAffinity (taskAffinity=""). You can also update the target SDK version (26) of the app to 29 or higher to fix this issue at platform level.

4. Resultados del Análisis Dinámico

Vulnerabilidad	Descripción	Impacto	Recomendación
Uso de Permisos de Ubicación en Segundo Plano	La app accede a la ubicación en segundo plano, lo cual podría violar la privacidad del usuario y consumir batería de forma innecesaria.	Riesgo de privacidad y consumo de batería	Limitar el uso de permisos en segundo plano
Abuso de Permisos Sensibles	Se utilizan permisos sensibles (ACCESS_FINE_LOCATION, INTERNET) sin justificación adecuada en el código de la aplicación.	Riesgo de abuso de permisos	Justificar el uso y restringir permisos.

4.1 Descripción de las Pruebas Dinámicas

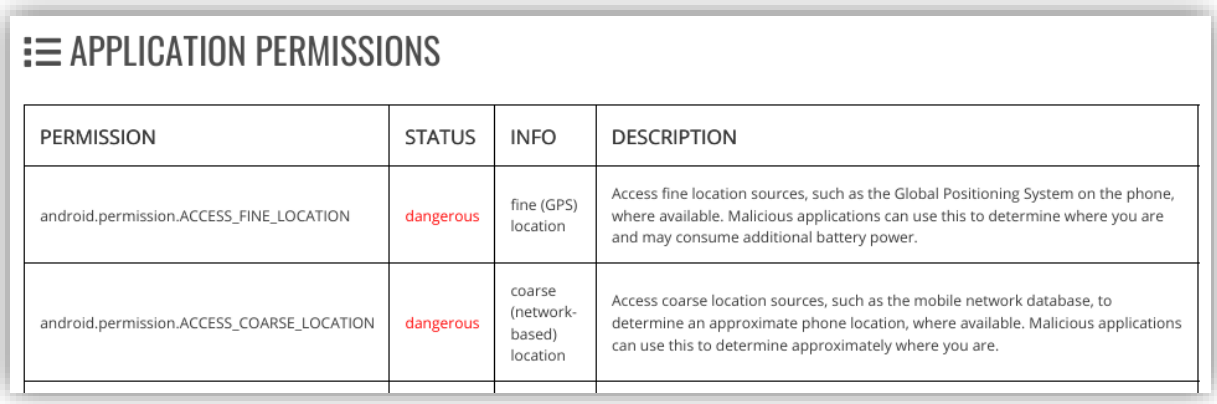
Permisos en Segundo Plano:

- Prueba: Monitoreamos el uso de permisos de ubicación mientras la app estaba en segundo plano.
- Resultado: La app continuó accediendo a la ubicación, generando un riesgo de privacidad.

Tráfico de Red:

- Prueba: Usamos un monitor de tráfico de red para observar las conexiones de la aplicación.
- Resultado: Detectamos tráfico no seguro en HTTP.

4.2 Captura de pantalla:



APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

5. Recomendaciones Generales

A continuación, se presentan recomendaciones clave para mitigar las vulnerabilidades encontradas:

- **Configurar Seguridad en Permisos:** Limitar el uso de permisos a solo las funcionalidades necesarias y justificar el acceso a permisos sensibles.
- **Implementar HTTPS:** Asegurarse de que todas las conexiones de red sean seguras mediante HTTPS para proteger los datos del usuario.
- **Actualizar la Configuración de Respaldo:** Desactivar el respaldo de datos para evitar el acceso no autorizado a la información de la app.

6. Conclusión

El análisis de vulnerabilidad ha revelado varias áreas críticas que deben mejorarse en GPSMapApp para cumplir con estándares de seguridad y privacidad. Las recomendaciones proporcionadas son esenciales para reducir riesgos y proteger los datos del usuario en futuras versiones de la aplicación.