SANTO®
TOMÁS

INSTITUTO PROFESIONAL
CENTRO DE FORMACIÓN TÉCNICA

Informe de Análisis de Vulnerabilidades de la Aplicación con Quixxi

Nombre Alumno: Josué Figueroa
Profesor: MANUEL MERINO PICEROS
Asignatura: Programación Android
Carrera: Ingeniería en Informática
Fecha: 23/10/2024

Índice

1. Introducción

Este informe presenta los resultados del análisis de seguridad realizado a una aplicación móvil Android que integra Google Maps. El análisis se llevó a cabo utilizando la herramienta Quixxi, con el objetivo de identificar posibles vulnerabilidades, evaluar la seguridad de la aplicación y proponer mejoras pertinentes para mitigar riesgos. Se analizaron aspectos relacionados con el almacenamiento de datos, privacidad, criptografía, interacción con la plataforma, calidad del código, y resiliencia

Resultado de análisis de la aplicación(GPS-JF):

MASVS	Issue	Severity	Assessment Status	CWE	Exploits	Can be fixed by Quixxi Shield	View Details
V2 Data Storage and Privacy	ADB Backup allowed	Medium	Fail	CWE-530, CWE-312	CVE-2017-16835		View Details
	Missing protection against screenshots & screensharing	Medium	Fail	CWE-200	CVE-2015-6630	FIXABLE BY Quixxi	View Details
	No blurring for the app in background	Medium	Fail	CWE-200	CVE-2015-6630	FIXABLE BY Quixxi	View Details
V3 Cryptography	Weak Java Hash Code implementation	Warning	Fail	CWE-327			View Details
V6 Platform Interactions	Improper Export of your Android Broadcast Receiver	High	Fail	CWE-927, CWE-925	CAPEC-499, CAPEC-501		View Details
V7 Code Quality and Build Settings	Debuggable App	Medium	Fail	CWE-215	CVE-2019-16273, CVE-2019-16272, CVE-2019-16241, CVE-2017-3750		View Details
	Debugging Information Provision	Medium	Fail	CWE-215	CAPEC-133, CVE-2018-6599	FIXABLE BY Quixxi	View Details
	Missing check for the download source	Low	Fail	CWE-610	CVE-2018-9582	FIXABLE BY Quixxi	View Details
V8 Resilience Requirements	Missing Native [C, C++] Code	Medium	Fail		CAPEC-190	FIXABLE BY Quixxi	View Details
	App allowed to run in a rooted device	Low	Fail		CVE-2017-4896	FIXABLE BY Quixxi	View Details
	App allowed to run in an emulator	Low	Fail			FIXABLE BY Quixxi	View Details

2. Análisis de Vulnerabilidades

El análisis se llevó a cabo siguiendo las recomendaciones del estándar OWASP (Open Web Application Security Project) y se evaluaron los siguientes puntos:

2.1 Almacenamiento de Datos y Privacidad (V2)

Vulnerabilidades encontradas: 3

Descripción: Se detectaron problemas relacionados con la privacidad de los datos, tales como permitir las copias de seguridad mediante ADB (Android Debug Bridge), falta de protección contra capturas de pantalla y uso compartido de pantalla, y la ausencia de desenfoque de la aplicación al estar en segundo plano.

CVE: CWE-530, CWE-312

Severidad: Media

V2 Data Storage and Privacy	ADB Backup allowed	Medium	Fail	CWE-530 , CWE-312	CVE-2017-16835
	Missing protection against screenshots & screensharing	Medium	Fail	CWE-200	CVE-2015-6630
	No blurring for the app in background	Medium	Fail	CWE-200	CVE-2015-6630

2.2 Criptografía (V3)

Vulnerabilidad encontrada: 1
Descripción: Implementación débil del código Hash de Java, lo que debilita la seguridad criptográfica de la aplicación.
CVE: CWE-327
Severidad: Advertencia

V3 Cryptography	Weak Java Hash Code implementation	Warning	Fail	CWE-327	

2.3 Interacciones con la Plataforma (V6)

Vulnerabilidad encontrada: 1

Descripción: Exportación incorrecta del receptor de difusión (Broadcast Receiver) de Android, lo cual puede permitir que componentes externos no autorizados accedan a funciones internas de la aplicación.

CVE: CWE-927, CWE-925

Severidad: Alta

V6 Platform Interactions	Improper Export of your Android Broadcast Receiver	High	Fail	CWE-927 , CWE-925	CAPEC-499 , CAPEC-501

2.4 Calidad del Código y Configuración de Compilación (V7)

Vulnerabilidades encontradas: 3

Descripción: Se detectó que la aplicación está configurada en modo depuración ("debuggable"), lo que puede exponerla a riesgos en entornos de producción. Además, falta la verificación de la fuente de descarga y se proporciona información sensible en los registros de depuración.

CVE: CWE-215, CWE-610

Severidad: Media a baja

V7 Code Quality and Build Settings	Debuggable App	Medium	Fail	CWE-215	CVE-2019-16273 , CVE-2019-16272 , CVE-2019-16241 , CVE-2017-3750
	Debugging Information Provision	Medium	Fail	CWE-215	CAPEC-133 , CVE-2018-6599
	Missing check for the download source	Low	Fail	CWE-610	CVE-2018-9582

2.5 Resiliencia (V8)

Vulnerabilidades encontradas: 3

Descripción: La aplicación permite su ejecución en dispositivos rooteados y emuladores, lo cual puede ser aprovechado por atacantes para analizar y modificar el comportamiento de la aplicación.

CVE: CWE-2017-4896

Severidad: Baja

V8 Resilience Requirements	Missing Native [C, C++] Code	Medium	Fail		CAPEC-190
	App allowed to run in a rooted device	Low	Fail		CVE-2017-4896
	App allowed to run in an emulator	Low	Fail		

3. Implementación de Mejoras

Para mitigar las vulnerabilidades encontradas, se proponen las siguientes acciones de mejora:

Deshabilitar ADB Backup: Implementar restricciones que impidan el respaldo de la aplicación mediante ADB.

Protección contra capturas de pantalla: Añadir mecanismos para evitar capturas de pantalla y el uso compartido de pantalla cuando la aplicación maneje datos sensibles.

Mejorar el manejo de criptografía: Sustituir el código hash de Java por algoritmos criptográficos más robustos.

Corregir exportación de componentes: Limitar la exportación de los Broadcast Receivers solo a los procesos internos de la aplicación.

Deshabilitar el modo depuración en producción: Asegurarse de que la configuración de la aplicación esté correctamente ajustada para entornos de producción.

Proteger la app contra ejecución en dispositivos rooteados: Implementar medidas de detección de root y bloquear el acceso si se detecta.

4. Recomendaciones de Seguridad

Es recomendable aplicar buenas prácticas de seguridad de manera continua para asegurar la robustez de la aplicación, tales como:

- Realizar auditorías de código regulares.
- Implementar autenticación segura en todas las conexiones de red.
- Utilizar cifrado de extremo a extremo para datos sensibles.
- Monitorear la aplicación en producción para detectar anomalías.

5. Conclusión

El análisis de seguridad identificó varias vulnerabilidades críticas y de mediana importancia en la aplicación. Implementar las mejoras propuestas permitirá reforzar la seguridad de la aplicación, proteger los datos de los usuarios, y cumplir con los estándares de seguridad móviles recomendados por OWASP. Se recomienda realizar pruebas continuas y una revisión periódica del estado de la seguridad de la aplicación.