Auditorías de Seguridad de Aplicaciones Android

Introducción

La evolución tecnológica y la amplia adopción de dispositivos móviles Android han incrementado significativamente el número de aplicaciones disponibles en el mercado. Este crecimiento ha traído consigo riesgos de seguridad que deben ser analizados mediante auditorías especializadas.

Siguiendo la lectura propuesta, en este informe se identificarán tres aplicaciones Android que actualmente presentan riesgos de seguridad, justificando su elección de acuerdo con los criterios recogidos en la metodología OWASP Mobile Top 10.

Aplicaciones Identificadas

1. TikTok

Justificación:

TikTok ha sido criticada por prácticas de recolección excesiva de datos, acceso indebido a funcionalidades del dispositivo y utilización inadecuada de los permisos de la plataforma. Investigaciones han revelado comunicaciones no suficientemente protegidas y almacenamiento de datos sensibles sin las debidas medidas de seguridad.

Amenazas OWASP implicadas:

- M1 – Uso inadecuado de la plataforma: acceso innecesario a funcionalidades del dispositivo.

- M2 – Almacenamiento inseguro de datos: almacenamiento local de datos sin la protección adecuada.

- M3 – Comunicación insegura: tráfico de red a servidores externos sin cifrado robusto en algunas versiones.

2. UC Browser

Justificación:
UC Browser ha sido objeto de controversia por enviar información de usuarios (como la localización y consultas de búsqueda) a servidores remotos sin el uso apropiado de mecanismos de cifrado, comprometiendo la privacidad de sus usuarios.

Amenazas OWASP implicadas:

- M2 – Almacenamiento inseguro de datos: gestión inadecuada de información local sensible.

- M3 – Comunicación insegura: transferencia de datos sin cifrado fuerte (HTTPS inconsistente).

- M5 – Cifrado insuficiente: uso de protocolos de cifrado obsoletos o mal implementados.

3. TurboVPN

Justificación:
TurboVPN, pese a promocionarse como una herramienta para proteger la privacidad, ha sido denunciada por compartir datos de usuarios con terceros y por deficiencias graves en los mecanismos de autenticación y autorización. Esto supone un riesgo directo para los usuarios que confían en la aplicación para proteger su identidad en línea.

Amenazas OWASP implicadas:

- M4 – Autenticación insegura: implementación débil en la autenticación de usuarios.

- M6 – Autorización insegura: control inadecuado sobre los accesos y privilegios.

- M3 – Comunicación insegura: tráfico de datos a través de canales no suficientemente protegidos.

Conclusiones

El análisis de estas aplicaciones demuestra que, a pesar de su popularidad o propósito declarado, muchas apps Android pueden comprometer seriamente la seguridad de los datos de los usuarios.

Aplicaciones como TikTok, UC Browser y TurboVPN presentan riesgos evidentes relacionados con almacenamiento inseguro, comunicación insegura, uso inadecuado de la plataforma y deficiencias en la autenticación y autorización, aspectos todos ellos recogidos en el proyecto OWASP Mobile Top 10.

Por ello, resulta fundamental realizar auditorías de seguridad periódicas y adoptar buenas prácticas de desarrollo y auditoría como las propuestas por la metodología OWASP Mobile Application Security (MAS).

Referencias

- OWASP Mobile Top Ten Project. OWASP. Disponible en: https://owasp.org/www-project-mobile-top-10/

- INCIBE (2023). Auditorías de seguridad de apps Android. Instituto Nacional de Ciberseguridad.

- Pradeo Security Research Center (2022). Mobile Threat Report: Popular Applications' Privacy and Security Issues. Disponible en: https://www.pradeo.com/blog/mobile-threat-report-popular-applications-privacy-and-security-issues