Rapport d’audit de sécurité Android

Auteur : Consultant Sécurité
Date : Septembre 2025

1. Introduction

Ce rapport présente les résultats de l’audit de sécurité réalisé sur une application Android sous forme d’APK.
L’objectif était d’identifier les vulnérabilités potentielles, d’évaluer la robustesse de l’application et de fournir des recommandations pour renforcer sa sécurité.

2. Méthodologie

Décompilation de l’APK

Outil utilisé : apktool

Commande :

```
apktool d app.apk -o out/apktool_out
```

Analyse statique

Fichiers étudiés : strings.xml, AndroidManifest.xml, code Smali

Recherche de clés/API, configurations risquées, communication non sécurisée.

Recompilation et signature

Rebuild avec apktool

Signature avec apksigner

Vérification via apksigner verify.

3. Résultats (Findings)

3.1 Secrets exposés

Preuve :

```
<string name="api_key">AIzaSy*********</string>
```

Risque : Élevé

Recommandation : Externaliser les clés API (Keystore Android) et régénérer la clé compromise.

3.2 Communications non sécurisées

Preuve :

```
const-string v0, "http://insecure-api.example.com"
```

Risque : Moyen

Recommandation : Forcer HTTPS et configurer la validation stricte des certificats.

3.3 Application en mode debug

Preuve :

<application android:debuggable="true" ... >

Risque : Élevé

Recommandation : Désactiver debuggable avant toute mise en production.

4. Preuves techniques

Recompilation réussie : rebuilt.apk généré

Signature appliquée : rebuilt_signed.apk

Vérification réussie :

apksigner verify --verbose rebuilt_signed.apk
Verified

5. Conclusion

L’application présente plusieurs vulnérabilités importantes :

Clés sensibles exposées

Communications non sécurisées

Application livrée en mode debug

Recommandations globales :

Mise en place d’une gestion sécurisée des secrets

Passage complet en HTTPS

Renforcement de la configuration Android avant publication

Intégration d’outils de scanning dans le pipeline CI/CD