Applications mobiles : l'inquiétante approche des compagnies aériennes

L'éditeur de solutions montpelliérain Pradeo a effectué un audit de sécurité de 50 applications mobiles de compagnies aériennes*.

Les apps étudiées permettent, entre autres, de réserver et acheter un billet d'avion, de scanner un passeport, de télécharger et afficher une carte d'embarquement…

La plupart de ces programmes ont donc accès à des données sensibles.

Près d'une application sur deux (49%) manipule ainsi des données de géolocalisation, photos ou contacts des utilisateurs. De surcroît, un tiers des applications envoient ces données sur le réseau, relève l'entreprise de sécurité mobile.

Or, le plus souvent, ces envois sont réalisés via des connexions non certifiées. Ainsi, les applis du panel utilisent en moyenne 14 connexions non sécurisées, selon le rapport.

L'expérience client risque également de pâtir des vulnérabilités repérées.

Top 10 des vulnérabilités de code

Le rapport fait état d'une moyenne de 21 vulnérabilités de code par application testée.

Or, les failles les plus souvent identifiées « exposent les applications au déni de service, à la fuite de données et aux attaques dîtes de 'l'homme du milieu' (man-in-the-middle) », a expliqué Pradeo dans un billet de blog.

L'éditeur livre le top 10 des vulnérabilités présentes dans les apps de l'échantillon :

1. Broadcast activity (98%)
2. DSQLite (94%)
3. Broadcast receiver (92%)
4. SQLC_password (90%)
5. Implicit intent (88%)
6. Broadcast service (86%)
7. d_JSenabled (78%)
8. d_external storage (66%)
9. d_webviewdebug (47%)
10. HandleSslError (16%)

**L'audit a été mené via le moteur d'analyse d'applications mobiles Pradeo Security durant la semaine du 20 mai 2019. Sont concernées des apps de compagnies aériennes d'Amérique du Nord, d'Europe de l'Ouest et d'Asie de l'Est, principalement.*

(crédit photo de une © shutterstock)