# United Airlines part à la chasse aux bugs avec des miles

L'appât du gain ne devrait pas être au rendez-vous des experts en sécurité habitués à concourir aux différents bounty program. Celui proposé par United Airlines est original à plus d'un titre. En premier lieu, le périmètre du terrain de jeu des hackers est très encadré. Pas question ici de contourner ou de pirater les systèmes embarqués des avions via le WiFi ou les écrans connectés de l'appareil, ni de s'en prendre au site interne de la compagnie.

Les chasseurs de failles devront se contenter du site officiel de United Airlines, de la version beta du site mobile, de l'application, du programme de fidélité. Les méthodes utilisées sont aussi strictement circonscrites, pas d'attaques en force brute, par déni de service, injection de code sur le système de production et bien évidement de tester son exploit sur les systèmes embarqués des avions.

## Des miles comme récompense

Côté récompense, la firme américaine ne versera pas d'argent mais des points de fidélité selon la criticité de l'exploit. Pour une faille permettant l'exécution du code à distance, United Airlines promet jusqu'à 1 million de miles, le contournement de l'authentification permet d'atteindre 250 000 milles et un cross-scripting une réserve de 50 000 miles. Pour en profiter, il faut bien évidement être inscrit au programme de fidélité de la compagnie.

Ce programme de chasse aux bugs s'inscrit dans un contexte particulier. Il y a quelques semaines un rapport du GAO (Governement Accountability Office) rapportait les risques importants sur les réseaux WiFi en vol et les communications utilisées par les avions. En écho à ce rapport, l'affaire Chris Robert a montré qu'il ne fallait pas plaisanter avec la sécurité aérienne. Cet expert en sécurité avait tweeté dans un vol de United Airlines qu'il allait pirater le réseau WiFi de l'appareil pour déclencher la chute des masques à oxygène. Un tweet qui selon lui était une blague mais qui lui a valu une discussion poussée avec le FBI et de se retrouver *persona non grata* sur les vols de la compagnie aérienne.

**A lire aussi :**

Espionnage : les Etats-Unis lancent des avions renifleurs de data mobile
Black Hat : un chercheur pirate les équipements satellites des avions via le WiFi