Sécurité : les hotspots Cisco victimes d'une vulnérabilité critique

Cisco est victime d'une nouvelle vulnérabilité de sécurité qui touche ses produits réseaux locaux (LAN) sans fil, rapporte ce mardi 25 août la société **AirMagnet**, spécialisée dans les réseaux sans fil. Selon elle, en cas d'exploitation, la faille permet de prendre le contrôle d'un point d'accès avec le risque de détourner les communications et de s'introduire sur le réseau de l'entreprise.

Selon AirMagnet, la faille touche **la fonction OTAP** (Over-the-Air-Provisioning). Cette fonctionnalité permet à un *hotspot* non connecté à un contrôleur Cisco « d'écouter » les communications des point d'accès Cisco voisins afin de repérer le contrôleur sans fil le plus proche et de s'y associer.

C'est au cours de cette phase de synchronisation qu'apparaît la vulnérabilité sous forme de deux éléments. Le premier verra la **fuite d'informations** depuis les points d'accès. Le deuxième entraîne un risque de défaut de configuration qui permettrait au hotspot d'être assigné autre part qu'au contrôleur Cisco, qui ce soit de manière accidentelle ou malveillante.

Pour l'heure, Cisco n'a fourni **aucun correctif**. AirMagnet déclare avoir alerté l'équipementier de l'existence de la vulnérabilité. En attendant, AirMagnet conseille de ne pas exploiter la fonction OTAP et de renforcer la sécurité de l'infrastructure sans fil à l'aide d'un système de détection d'intrusion pour prévenir les risques d'attaques ou d'espionnage. Comme ceux que propose AirMagnet, notamment.