Le standard WPS sur les routeurs WiFi piraté plus rapidement

Dominique Bongard est un spécialiste du reverse ingénierie et fondateur de la la société Suisse 0xcite et il a réalisé une attaque sur des routeurs WiFi via WPS. La fonction **WiFi Protected Setup** est un standard permettant d'établir des connexions et de configurer un réseau sans fil facilement et en toute sécurité. Cette connexion sécurisée peut se faire soit via un bouton pressoir ou soit via **un code PIN à 8 chiffres**.

Pour sa démonstration, il s'est appuyé sur l'absence ou la faiblesse de la technique de randomisation (affectation aléatoire) pour obtenir suffisamment d'information pour deviner les codes PIN des routeurs par des calculs hors ligne. Cette méthode évite une attaque en force brute, c'est-à-dire en générant l'ensemble des hypothèses pour trouver la bonne. Le spécialiste explique ainsi qu'une attaque menée en 2011par **Stefan Viehböck** nécessitait jusqu'à 11 000 suppositions pendant 4 heures pour accéder aux routeurs (en découpant le code PIN en plusieurs petits paquets). Avec son procédé, Dominique Bongard se vante, « *il faut une seconde. Ce n'est rien, un coup et c'est terminé* ».

Une génération de clé pas assez aléatoire

Selon Ars Technica, le spécialiste a indiqué que le problème réside dans l'implémentation de WPS de deux fabricants de puces WiFi dont **Broadcom**. L'autre constructeur n'a pas été nommé pour lui laisser du temps pour corriger le bug. De nombreux équipementiers utilisent l'implémentation standard du WPS pour leur logiciel sur les routeurs. Or, Dominique Bongard affirme que le firmware de Broadcom disposait d'une mauvaise répartition aléatoire, tandis que le second équipementier utilisait un canal éliminant toute affectation aléatoire.

Interrogé sur ce problème de sécurité, **la WiFi Alliance** en charge du standard WPS n'est pas en mesure de confirmer l'étendue du problème. La porte-parole de l'association, **Carol Carruba**, a indiqué « *qu'il est probable que le problème réside dans les implémentations spécifiques du fournisseur plutôt que sur la technologie elle-même. Comme la recherche ne permet pas d'identifier les produits concernés, nous ne savons pas si tous les périphériques WiFi certifiés sont touchés* ».

crédit photo © mtkang – shutterstock

A lire aussi :

Un outil permet d'exploiter la faille WPS des bornes d'accès WiFi

Le protocole WPS des bornes WiFi n'est pas sûr