Le protocole WPS des bornes WiFi n'est pas sûr

Alerte générale pour toutes les personnes disposant d'une borne d'accès sans fil proposant un bouton de connexion rapide.

Le protocole de sécurité WPS (*Wi-Fi Protected Setup*) présenterait en effet une faille béante. Selon **Stefan Viehböck**, chercheur indépendant et découvreur du pot aux roses, le phénomène touche un large éventail de produits génériques, expliquent nos confrères d'*ITespresso*.

Netgear, Belkin, D-Link et Buffalo sont quelques-uns des constructeurs incriminés à cette occasion. Quand bien même les différentes déclinaisons du WPA ne sont pas concernées, cette vulnérabilité dépasse la fragilité d'ores et déjà avérée de la protection WEP.

Pour mémoire, le WPS dispense de la saisie d'un mot de passe à la connexion, sans pour autant nécessiter d'appairage préalable, via une interface matérielle (un bouton situé sur le routeur) ou un identifiant unique assigné par un constructeur à chacun de ses terminaux connectés (comparable au filtrage d'adresses MAC).

Un procédé simple… trop simple

Une telle simplification des démarches offre une flexibilité accrue dans l'exploitation de réseaux domestiques en contrepartie ouverts aux quatre vents. D'autant plus que le protocole mis à défaut se base sur un artifice qui relève de l'aberration. Généré aléatoirement, le code PIN à 8 chiffres qui résulte d'une opération d'association offre en théorie 10^8 combinaisons possibles, soit 100 millions. Or, le dernier élément de cette série agit comme une simple clé de validation, tel le dernier segment constitutif d'un numéro de Sécurité sociale. Ce qui, à en croire les assertions de Sophos, ramène à 10^7 (10 millions) le nombre réel de combinaisons.

Plus contrariant, la transmission des bits de données ainsi acquis s'effectue en deux fois. Le système de vérification actuellement en place ne contrôle que l'une des deux moitiés envoyées séparément, soit 10^4, voire 10^3 possibilités. Dans l'absolu, il n'est alors plus qu'une question d'heures pour s'immiscer sur l'un des canaux d'émission du routeur visé, pour y injecter quelques paquets et passer outre la clé de sécurité.

Parmi les protections possibles contre cette faille, le chercheur préconise une désactivation du protocole WPS.