Sécurité : une backdoor découverte dans des routeurs Linksys et Netgear

Selon l'ingénieur en sécurité français **Eloi Vanderbeken** (qui se décrit comme un spécialiste du reverse engineering), plusieurs routeurs sans-fil Linksys et Netgear renferment une backdoor. Alors qu'il tentait d'accéder à son interface d'administration après avoir oublié le mot de passe, Eloi Vanderbeken a découvert une faille de sécurité sur son routeur Linksys WAG 200G, faille permettant d'**utiliser un port 'exotique' (le 32764) pour commander à distance le matériel**.

Prise de contrôle totale

« *J'avais perdu le mot de passe d'accès et interdit l'accès à la console depuis le WiFi, seul accès dont je disposais alors*, explique Eloi Vanderbeken, joint par la rédaction. *Je me suis alors intéressé aux ports non utilisés du routeur et je suis tombé sur ce port 32764. Les réponses que j'ai trouvées sur Google à ce propos ne m'ont pas satisfait. J'ai donc décidé de creuser* ». Et l'ingénieur de découvrir que, via ce port, le routeur **répond à une série de 13 commandes permettant de prendre totalement la main sur la machine**. « *Par exemple, de lire et modifier la configuration, d'exécuter des commandes, de changer le mot de passe admin, de flasher le firmware, etc.* », énumère Eloi Vanderbeken.

La publication de cette faille a permis de découvrir **d'autres modèles affectés** : Netgear DM 111Pv2, Linksys WAG 320N, Linksys WAG 54G2, DGN1000 Netgear N150 et Diamond DSL 642WLG. Une dizaine d'autres routeurs provenant des deux fabricants sont eux aussi suspectés de renfermer la porte dérobée (voir la liste ici). Eloi Vanderberbeken suspecte que cette faille provient d'un sous-traitant des deux constructeurs, **SerComm**. Ce dernier pourrait, par exemple, avoir utilisé le port 32764 pour des tests lors du développement des modules qu'il fournit aux constructeurs.

Voir aussi

Silicon.fr étend son site dédié à l'emploi IT
Silicon.fr en direct sur les smartphones et tablettes