Alerte : Des millions de routeurs domestiques peuvent être attaqués à distance | Le Net Expert Informatique

Une faille dans le driver NetUSB permet à un pirate de prendre le contrôle total de l'équipement et d'y installer, par exemple, des malwares. Pour l'instant, seul TP-Link a fourni un correctif.

Netgear, TP-Link, Trendnet, Zyxel… Si vous possédez un routeur domestique de l'une de ces marques, il est probable que vous ayez un problème de sécurité. La plupart de ces routeurs disposent en effet d'une fonctionnalité théoriquement assez pratique, à savoir le partage en réseau d'une connexion USB. Concrètement, vous connectez un équipement en USB sur votre routeur – un disque dur par exemple – et celui-ci devient alors accessible à distance au travers du réseau. Beaucoup de ces routeurs s'appuient pour cela sur un module logiciel nommé « NetUSB », développé par le fournisseur taiwanais KCodes.
Le problème, c'est qu'il existe dans ce module une faille qui permet à une personne mal intentionnée de faire crasher le routeur ou d'y exécuter n'importe quel code. Et donc d'en prendre possession pour, par exemple, y installer des malwares. Cette vulnérabilité a été découverte par les chercheurs en sécurité de la société autrichienne SEC Consult. Elle repose sur une erreur de codage : quand le nom de l'ordinateur qui souhaite se connecter à distance est supérieur à 64 caractères, le module NetUSB génère un dépassement de mémoire tampon et le fait planter. Pire : comme ce module est exécuté au niveau du noyau Linux du routeur, cette faille permet d'accéder au plus haut niveau de privilège. Plutôt pratique pour un pirate.

Exemple de routeur vulnérable.

Attaque par Internet
Certains d'entre vous se diront que ce n'est pas si grave que cela, car il faut déjà pouvoir rentrer dans le réseau domestique pour réaliser cette attaque. Mais cela n'est pas toujours vrai. Les chercheurs de SEC Consult ont trouvé que pour un certain nombre de routeurs, les connexions NetUSB étaient accessibles par Internet, peut-être en raison d'une mauvaise configuration. Par ailleurs, il s'avère que la procédure d'authentification utilisée pour initier une connexion avec NetUSB est totalement inutile : « les clés AES sont statiques et peuvent être trouvées dans le driver », expliquent les chercheurs. En d'autres termes, lorsque le routeur expose sa fonctionnalité NetUSB sur le web, un pirate pourra s'y introduire sans problème.
Une rapide recherche a montré qu'au moins 26 fabricants de routeurs utilisent le logiciel de KCodes dans au moins 92 produits. Ce qui représente certainement plusieurs millions de clients dans le monde. Contacté par les SEC Consult, KCodes n'a fait aucun commentaire. Que faut-il faire pour se protéger ? Seul TP-Link a développé, à ce jour, un correctif qu'il diffusera progressivement dans ses différents modèles. Dans certains équipements, il est possible, par ailleurs, de désactiver le partage de connexion USB. Les clients de Netgear, en revanche, ne pourront rien faire. Le fabricant a indiqué d'emblée ne pas pouvoir produire de patch, et qu'il était impossible de désactiver la fonction de partage. Il ne reste alors qu'une seule solution : la prière.

Source : http://www.01net.com/editorial/655187/des-millions-de-routeurs-domestiques-peuvent-etre-attaques-a-distance/