# Des routeurs WiFi Netgear à la portée des pirates

Le centre de sécurité du Department of Homeland Security américain (US-CERT) lance une alerte concernant 2 routeurs Wifi de marque Netgear affectés par une vulnérabilité très sévère. Les modèles concernés, les R6400 et R7000, sont touchés par une faille de type injection de commandes. « *Exploiter cette vulnérabilité est trivial* », explique le CERT dans son alerte. Et d'ajouter : « *les utilisateurs qui en ont la possibilité devraient réfléchir sérieusement à l'arrêt de l'utilisation de ces machines tant qu'un correctif n'est pas disponible* ». Ce qui n'est pas le cas à ce jour…

Pour infecter un des routeurs, il suffit qu'un assaillant persuade un utilisateur de cliquer sur un lien spécialement conçu (de type http:// < router_IP >/cgi-bin/;COMMAND qu'il est possible de masquer dans une URL raccourcie). Ce qui lui permet, potentiellement, de prendre le contrôle total du routeur ciblé.

## Cible idéale pour Mirai

Le CERT-US a décidé de lancer cette alerte publique après qu'un utilisateur se faisant appeler Acew0rm a publié sur une base de données de codes d'exploitation des informations relatives au détournement des routeurs Netgear. Le danger ? Que ces boîtiers soient enrôlés dans un botnet, un réseau de machines zombies permettant à un pirate de lancer des attaques par déni de service distribué (DDoS). Au cours des dernières semaines, des cybercriminels ont ainsi détourné des modems Eir ainsi que des routeurs AMG et D-Link au sein des réseaux de Deutsche Telekom en Allemagne et de TalkTalk et Postal Office en Grande-Bretagne. Des machines qui auraient été infectés par Mirai, un malware qui se répand sure un grand nombre d'objets connectés pour lancer de puissants DDoS. Un opérateur de botnet Mirai a ainsi récemment revendiqué plus de 3 millions de machines zombifiées.

## Le R8000 aussi

Selon l'alerte du CERT-US, la faille concerne le R7000 équipé du firmware en version 1.0.7.2_1.1.93 et le R6400 avec la version 1.0.1.6_1.0.4 du firmware. Le centre du Homeland Security indique toutefois que les moutures antérieures du logiciel interne sont peut-être également concernées par la faille. Sur le site communautaire *Reddit*, un internaute précise que l'exploit fonctionne également sur les modèles R800, ce que mentionne également le CERT-US, dans une mise à jour de son alerte. Qui indique : « *d'autres modèles pourraient aussi être touchés* ».

Pour ceux qui ne pourraient mettre hors service temporairement ces machines, le centre de sécurité américain préconise la désactivation du serveur Web sur les routeurs, rendant inaccessible l'interface d'administration des boîtiers après redémarrage. Mieux que rien. Pour l'heure, Netgear dit enquêter sur le sujet et a ouvert une page Web dédiée qu'il entend mettre à jour au fil des résultats de ses investigations.

**A lire aussi :**

A louer : un botnet Mirai de 400 000 objets pour lancer des DDoS

900 000 boxes Internet de Deutsche Telekom mises HS par un piratage

Sécurité et IoT : pourquoi le pire est encore à venir