# Cinq failles de sécurité majeures dans des modem-routeurs Arris

Très utilisés aux Etats-Unis, notamment en marque blanche par les fournisseurs d'accès comme AT&T, plusieurs modem-routeurs **Arris** sont affectés de cinq failles de sécurité majeures.

La plupart permettent de prendre le contrôle du boîtier et de le transformer, par exemple, en machine à spam ou à détourner les connexions.

Absent du catalogue en ligne d'Arris, les références des routeurs se destinent avant tout aux fournisseurs d'accès Internet de type opérateurs télécoms.

Selon Nomotion, firme de conseils et de développement applicatifs spécialisés en sécurité, la première vulnérabilité démontre une négligence difficilement pardonnable. Mais la firme de sécurité ne se prononce pas sur l'origine de la faille. Celle-ci existe peut-être depuis la conception des routeurs comme elle peut avoir été introduite par le fournisseur d'accès.

Dans tous les cas, *« il incombe au fournisseur d'accès Internet de s'assurer que son réseau et son équipement fournissent un environnement sécurisé à leurs utilisateurs finaux »*, considère Nomotion sur sa contribution de blog.

## Des identifiants codés en dur et publiés en ligne

La première vulnérabilité répertoriée est présente dans la plus récente mise à jour du firmware maison (9.2.2h0d83) et touche les modèles NVG589 et NVG599. Elle permet l'accès au modem alors que les identifiants de connexion sont codés en dur. Quiconque les connait peu avoir accès au routeur. Ce qui est désormais le cas de tout le monde potentiellement puisque Nomotion n'a pas hésité à les publier sur sa page.

Les identifiants donnent notamment accès au cshell, une interface qui permet de changer l'identifiant Wi-Fi du routeur, modifier la configuration du réseau, changer le firmware à partir d'un fichier disponible sur n'importe quel serveur TFTP (Trivial File Transfert Protocol) qui ne nécessite pas d'identification, et même *« contrôler ce qui semble être un module de noyau dont le seul but semble être d'injecter des publicités dans le trafic Web non chiffré de l'utilisateur »*.

La deuxième faille se rapporte à un serveur HTTPS, *« à l'utilité inconnue »*, tournant sur le port 49955 du modem NVG599. La encore, son accès est des plus simple puisque l'identifiant « tech » y donne accès sans même à avoir à saisir de mot de passe.

La troisième vulnérabilité permet d'injecter des commandes sur « caserver », un serveur HTTPS tournant également sur le port 49955 pour télécharger une nouvelle image du firmware, consulter la base de données interne (SDB) et en changer la configuration.

## 220 000 routeurs affectés

La quatrième faille touche le port 61001 qui apportera à l'attaquant *« une pléthore de données utiles sur l'appareil »* dont le numéro de série du boîtier.

La cinquième brèche permet de contourner le firewall en exploitant le service d'écoute depuis le port 49152 et d'ouvrir une connexion proxy TCP. Un bon moyen de pouvoir exploiter les quatre autres failles même si l'utilisateur pense être protégé en activant son firewall.

*« Tous les appareils AT&T étudiés ont ce port (49152) ouvert et a répondu aux sondes »*, indique la firme de sécurité.

Pour l'heure, les failles ne sont pas exploitées, selon les chercheurs. Un calme apparent qui risque de ne pas durer après la révélation de Nomotion.

La société publie des instructions pour permettre le blocage des accès aux backdoors et corriger quelques certaines failles. Pas moins de 220 000 boîtiers Arris sont concernés par une des failles, selon les experts en sécurité.

---

**Lire également**
**Des routeurs WiFi Netgear à la portée des pirates**
**La liste des routeurs Cisco infectés par SYNful Knock s'allonge**
**Des pirates injectent du porno dans les tags de Google Analytics**

**crédit photo © Morrowind – shutterstock**