Une faille critique cible des milliers de routeurs ASUS

À la mi-mars 2025, GreyNoise a identifié une campagne d'attaques ciblant plus de 9 000 routeurs ASUS (RT-AC3100, RT-AC3200, RT-AX55), baptisée « AyySSHush ».

Les pirates peuvent-ils transformer nos routeurs ASUS en bots invisibles pour des attaques massives ?

Ils exploitent une vulnérabilité d'injection de commandes (CVE-2023-39780) et utilisent des attaques par force brute pour installer une porte dérobée persistante. Cette backdoor, stockée dans la mémoire NVRAM, active un service SSH sur un port non standard et désactive les journaux pour rester indétectable. Cela permet aux pirates de garder le contrôle du routeur même après mises à jour ou redémarrages, formant potentiellement un botnet mondial.

Une campagne parallèle, *ViciousTrap*, semble liée et cible également d'autres équipements réseau comme des NAS et des passerelles VPN.

Pour se protéger, il est crucial de mettre à jour le firmware, vérifier le port TCP 53282, bloquer les IP malveillantes (101.99.91[.]151, 101.99.94[.]173, 79.141.163[.]179, 111.90.146[.]237) et réinitialiser le routeur si nécessaire. En agissant ainsi, les utilisateurs peuvent prévenir l'exploitation de cette faille et limiter le risque de rejoindre involontairement un botnet.

Sources :

https://www.it-connect.fr/botnet-ayyysshush-une-porte-derobee-ssh-ajoutee-sur-plus-de-9-000-routeurs-asus/

https://www.macg.co/materiel/2025/05/un-malware-particulierement-resistant-infecte-des-milliers-de-routeurs-asus-301681

Outil de sourcing : Google Alerts