Sécurité : Huawei ne corrigera pas les failles de ses routeurs Wimax

Le 1er juillet 2015, le chercheur en sécurité **Pierre Kim** découvrait des vulnérabilités dans plusieurs routeurs de Huawei et en informait aussitôt l'équipementier chinois. Notamment pour savoir si et quand d'éventuels correctifs seraient livrés. Le 18 novembre, après plusieurs échanges, Huawei répondait qu'aucun patch ne serait développé pour combler les failles de sécurité en question. *« Les routeurs sont arrivés en fin de vie et Huawei n'en assurera plus le support désormais »*, a confirmé le fournisseur d'équipements réseau qui, en conséquence, *« encourage ses clients à éliminer les modèles existants non pris en charge et à utiliser de nouveaux routeurs. »* L'obsolescence par les failles…

> *Huawei Wimax routers vulnerable to multiple threats #infoleak #sessionhijacking #CSRF #IoT #EoL https://t.co/MZT9A3PqCW*
>
> *— Pierre Kim □□□ □ (@PierreKimSec) 30 Novembre 2015*

Remplacer lesdits routeurs est par ailleurs plus facile à dire qu'à faire. Surtout quand les clients concernés n'ont pas été alertés jusqu'à ce jour. Au moins six modèles EchoLife sont concernés par la vulnérabilité (EchoLife BM626 WiMAX CPE, BM635 WiMAX CPE, BM632 WiMAX CPE, BM631a WiMAX CPE, BM632w WiMAX CPE, BM652 WiMAX CPE). Et 8 autres pourraient l'être car ils partagent le même firmware. Le modèle BM626e est une «□box□» Wimax notamment exploitée par l'opérateur MTN en Côte d'Ivoire. *« Il est disponible dans un certain nombre de pays qui fournissent Internet avec un réseau Wimax »*, ajoute Pierre Kim sur sa page de blog. Notamment en Iran, Irak, Libye, aux Philippines, à Bahrain et en Ukraine. Après avoir notifié CERT.org des vulnérabilités, le chercheur les a rendues publiques le 1er décembre.

Portes grandes ouvertes

Selon Pierre Kim, les routeurs vulnérables offrent un accès relativement trivial à un attaquant qui pourra potentiellement accéder aux appareils connectés au réseau de la victime. D'une part, disponible sans authentification par simple adresse IP, la page d'accueil du boîtier contient des informations importantes dont les configurations Wimax, réseau, Wifi et SIP. L'attaquant peut alors profiter d'une gestion en cours sur le routeur pour accéder aux paramètres d'administration depuis un réseau local ou sans fil si le protocole HTTP est ouvert dans l'interface WAN. Le tout sans authentification. *« La session admin id (« SID ») peut être récupérée depuis de multiples pages Web sans authentification »*, écrit le chercheur. Notamment la page security.html qui contient une session d'identification valide à partir des sources Javascript, disponibles sans authentification.

Autant dire que la porte est grande ouverte. Et qu'elle n'est pas prête de se refermer puisque les routeurs en question sont distribués aux utilisateurs finaux (particuliers ou entreprises) par des fournisseurs d'accès seuls à même d'appliquer des correctifs que ne fournira de toute façon pas son constructeur. Avec le risque que, au-delà d'essayer de pénétrer le réseau local de l'utilisateur, les attaquants rattachent les routeurs vulnérables à un *botnet* en vue de lancer des attaques DDoS,

par exemple. Les routeurs résidentiels ou de petites entreprises constituent souvent une cible de choix pour les cyber-criminels. Particulièrement les «vieux» modèles qui ne sont plus supportés ou ceux qui ne sont pas mis à jour par leurs exploitants.

Lire également
Sécurité : 14 routeurs Cisco victimes d'un firmware IOS corrompu
Recrudescence d'attaques DDoS depuis de «vieux» routeurs
Les routeurs WiFi, de vraies passoires en matière de sécurité

crédit photo © i3d – shutterstock