

**Alerte : Une faille permet
aux hackers de contrôler les
connexions internet des
particuliers**

| | |
|---|---|
| ✖ | Alerte : Une faille permet aux hackers de contrôler les connexions internet des particuliers |
|---|---|

Les chercheurs F-Secure viennent de mettre à jour une faille critique présente sur certains des routeurs Inteno. Cette vulnérabilité est assez importante pour permettre à un pirate de prendre le contrôle total de l'appareil de la victime et des communications internet. Cette découverte met en lumière les problématiques de sécurité propres aux routeurs.

La vulnérabilité récemment détectée permet au pirate d'installer son propre firmware sur l'appareil, qui continuera, en apparence, à fonctionner comme avant...mais en coulisses, des backdoors et autres fonctionnalités pirates feront leur apparition. Le hacker sera capable de lire tout le trafic non-chiffré passant par le routeur : non seulement les communications appareil-internet, mais aussi celles établies entre deux appareils. Il pourra également manipuler le navigateur de la victime afin de la rediriger vers des sites malveillants.

« En remplaçant le firmware, le pirate peut changer n'importe quelle règle du routeur », explique Janne Kauhanen, Cyber Security Expert chez F-Secure. « Vous regardez du contenu vidéo stocké sur un autre ordinateur ? Alors, le pirate y a lui aussi accès. Vous mettez un jour un autre appareil à partir du routeur ? Pourvu que l'appareil en question ne renferme pas d'importantes vulnérabilités, sinon le pirate pourra également s'en saisir. Bien entendu, le trafic https est chiffré. Les pirates n'y auront pas accès facilement. Ils peuvent néanmoins vous rediriger systématiquement vers des sites malveillants afin d'installer des malware sur votre machine. »

« Le type de routeur en question reçoit des mises à jour firmware depuis un serveur associé au fournisseur d'accès de l'utilisateur. Problème : les routeurs vulnérables ne vérifient pas si la mise à jour est valide, ni si elle vient de la bonne source. Un pirate qui a déjà eu accès au trafic circulant entre le routeur et le serveur de mise à jour du FAI (par exemple, en accédant à la distribution réseau de l'immeuble où se trouve l'appartement) peut installer son propre serveur de mises à jour. Il peut ensuite installer son firmware malveillant.

Les chercheurs expliquent qu'il ne s'agit que de la partie émergée de l'iceberg en matière de sécurité routeurs. Les ordinateurs sont de mieux en mieux protégés mais les utilisateurs ignorent souvent que le routeur peut être lui aussi vulnérable.

« C'en est ridicule de constater à quel point les routeurs vendus sont peu sécurisés », explique Janne Kauhanen. « Nous trouvons des vulnérabilités routeurs en permanence. Les firmware utilisés par les routeurs et les objets connectés sont mal conçus. L'aspect sécurité est négligé tant par les fabricants que par les clients. Personne n'y porte attention, si ce n'est le pirate, qui utilise les vulnérabilités pour détourner le trafic internet, voler des informations, répandre des malware. »

La vulnérabilité détectée, bien que sévère, n'est pas immédiatement exploitable. Un pirate doit avoir déjà acquis une certaine position sur le réseau, en réalisant une incursion entre le routeur et le point d'entrée internet. Les routeurs concernés sur les Inteno EG500, FG101, DG201. D'autres modèles sont probablement concernés....[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : F-Secure : Une nouvelle faille, permettant aux hackers de contrôler les connexions internet des particuliers, révélée sur plusieurs routeurs – Global Security Mag Online