Caméras Foscam IP : de nombreuses failles rendent les appareils et les réseaux vulnérables aux cyber attaques

Les caméras IP non-sécurisées sont l'un des nombreux exemples d'objets connectés vulnérables face aux cyber menaces.

Rueil Malmaison, le 7 juin 2017 - F-Secure a découvert plusieurs failles sur deux caméras IP de Foscam. En exploitant ces vulnérabilités, détaillées dans un rapport, les pirates peuvent prendre le contrôle à distance sur l'appareil, des flux vidéo et des fichiers téléchargés depuis un serveur intégré. Si l'appareil se trouve sur un réseau local, le pirate peut accéder au réseau en question, et peut utiliser la caméra pour procéder à des attaques DDos ou à d'autres activités malveillantes.

« Ces failles permettent aux hackers de faire plus ou moins tout ce qu'ils désirent », explique **Harry Sintonen**, Senior Security Consultant chez F-Secure. Il a lui-même découvert ces vulnérabilités. « Ces failles sont très sérieuses. Un pirate peut les exploiter une par une, ou toutes à la fois, pour disposer de droits d'accès supplémentaires concernant l'appareil ou le réseau. »

Cette découverte vient s'ajouter à la longue liste d'objets connectés ou « intelligents », qui ne sont pas assez sécurisés pour faire face aux cyber attaques actuelles. Des voitures intelligentes, des caméras CCTV, des bouilloires et encore des routeurs se sont déjà avérés particulièrement peu sécurisés. Les dangers encourus sont devenus encore plus évidents après les ravages du botnet Mirai, qui s'est emparé des caméras et boîtiers DVR non-sécurisés. Cette attaque DDoS, qui a eu lieu en octobre dernier, est la plus importante qu'ait jamais connu internet.

Au total, 18 vulnérabilités ont été répertoriées. Les pirates peuvent infecter les appareils de différentes manières. La méthode d'identification non-sécurisée, codée « en dur », leur permet d'obtenir facilement les droits d'accès utilisateurs. Le logiciel ne restreint pas non plus l'accès aux fichiers critiques : les hackers peuvent ainsi les modifier avec leurs propres commandes. Il leur est également possible de réaliser des injections de commandes à distance, de mener des attaques XSS, de générer des dépassements de tampon, ou encore de forcer les mots de passe. Le pirate peut obtenir l'accès au menu principal, prendre le contrôle de l'appareil et l'utiliser comme pivot de son réseau.

« La cyber sécurité a été ignorée au moment de la conception », explique Harry Sintonen. « La principale préoccupation des développeurs a été de concevoir ces produits rapidement, pour les mettre sur le marché le plus vite possible. De nombreux principes de sécurité ont été ignorés, ce qui met les utilisateurs et leurs réseaux en danger. Ironie du sort : ces objets sont vendus en tant que dispositifs supposés mieux sécuriser votre environnement physique ! En retour, votre environnement virtuel est, lui, rendu particulièrement vulnérable. »

Le fabricant chinois Foscam propose de nombreux modèles de caméras IP. Certaines sont proposées en marque blanche et vendus sous d'autres noms, notamment OptiCam. Les deux modèles étudiés par Harry Sintonen sont les suivants : l'OptiCam i5 HD et la Foscam C2. D'après Sintonen, il est probable que les failles présentes sur ces caméras existent sur d'autres appareils fabriqués par Foscam.

Harry Sintonen recommande d'isoler ces caméras du reste du réseau, afin de ne pas mettre en danger l'ensemble de l'infrastructure en cas d'attaque. « Changer le mot de passe par défaut est aussi un principe de

base », ajoute-t-il. « Malheureusement, avec ces appareils, la méthode d'identification permet au pirate de contourner le mot de passe même si celui-ci a été modifié. »

Foscam a été informé de ces failles il a déjà plusieurs mois mais, à ce jour, aucun patch n'est encore disponible.