# Objets connectés : une moyenne de 5 failles par objet


Objets connectés : une moyenne de 5 failles par objet

**9271 vulnérabilités majeures découvertes dans le firmware de 185 « objets de l'internet », principalement des routeurs, modems DSL/câble, téléphone IP, caméras de surveillance sous IP etc.**

C'est le résultat brut de l'étude signée Andrei Costin et Aurélien Francillon d'Eurecom avec le concours d'Apostolis Zarras de l'Université de Bochum.
Réduire l'étude de ces trois chercheurs en quelques chiffres ne rend pas justice au travail effectué. En fait, son aspect le plus intéressant porte surtout sur l'automatisation et le travail à grande échelle de cette chasse au bug, grâce à la mise en place d'un environnement d'émulation.
La machine virtuelle est adaptée aux principaux systèmes et matériel du commerce, et les firmware chargés puis épluchés de manière dynamique les uns après les autres. Une sorte de « VM de torture » reproduisant au mieux l'environnement d'exécution.
Autre point important, cette recherche s'est limitée (sic) aux simples interfaces Web d'administration et de paramétrage qui sont en général intégrées dans le moindre des objets IoT. Et qui, pourrait-on ajouter, constituent le ventre mou de ces systèmes embarqués depuis des lustres. En d'autres mots, il n'est pas question ici des failles matériel, des trous Wifi/bluetooth/DECT, bref, de ce qui sort du volet « httpd » de ce travail. Il y a fort à parier que si l'analyse avait pu s'étendre à ces aspects, le nombre de défauts recensés aurait été probablement doublé.
Mais ce genre de tests est nettement moins susceptible de pouvoir être automatisé. Les armes de chasse sont classiques : Arachni, Zed Attack Proxy, w3af, ce qui n'interdit pas à tout chercheur souhaitant continuer ce travail d'y ajouter Metasploit ou Nessus.
L'environnement lui-même, Qemu, a été retenu en raison du nombre important de processeurs supportés : Arm, Mips, Mipsel, Axis Cris, bFLT, PowerPC, X86 et même Nios II d'Altera.
Certains cœurs échappent à ce crible, tels les processeurs spécifiques de Dlink ou un Risc 32 bits peu répandu, le Arctangent A5.
Plus de la moitié des objets utilisant un ARM ont été vulnérables à un Chroot et une attaque Web, entre 17 et 21 % pour les systèmes à base de MIPS, et un peu moins de 30 % pour les IoT avec moteur Mipsel.
Les vulnérabilités les plus fréquemment rencontrées sont : XSS (5000 sur les 9271 recensées), manipulation de fichiers (1129), exécution de commandes arbitraires (938), ajout de fichiers (513), divulgation de fichiers (461), injection SQL (442)…

La confiance dans l'IoT, ça se mérite. Toutefois, précisent les trois chercheurs, il est des domaines où la sécurité est prise nettement plus au sérieux.
C'est notamment le cas de boîtier de télévision payante, par câble ou satellite. Probablement en raison des conséquences de pertes économiques directes qu'un défaut de sécurité provoquerait immédiatement, certainement aussi conséquemment aux multiples hacks qui, depuis plus de 20 ans, ont conduit ces intégrateurs à s'engager dans une course au blindage antipirates.
Comme quoi, c'est pas la sécurité qui manque, dans le domaine de l'Internet des Objets, c'est la menace financière.

---

Réagissez à cet article
Source : http://www.cnis-mag.com/iot-une-moyenne-de-5-failles-par-objet.html