www.silicon.fr

Date : 13/08/2014

Sécurité : les firmwares des terminaux connectés sont des passoires

Par : Reynald Fléchaux

Les firmwares des imprimantes, routeurs et autres caméras de surveillance sont loin de bénéficier du niveau de sécurité requis, confirme une étude française. Qui s'est penchée sur pas moins de 32 000 firmwares.

Les firmwares des systèmes embarqués (imprimantes, routeurs, périphériques, caméras de vidéo-surveillance, systèmes Scada, voitures connectées…) sont bien souvent soupçonnés de servir de porte d'entrée aux pirates. **Des chercheurs d'Eurecom**, une école d'ingénieurs en télécommunications située à Sophia Antipolis, viennent de confirmer l'ampleur du problème dans ce qu'ils présentent comme la « *première étude publique à grande échelle sur les images de firmwares* ». Les quatre chercheurs (Andrei Costin, Jonas Zaddach, Aurélien Francillon et Davide Balzarotti) ont réuni 32 000 images de firmwares et analysé plus de 26 000 (dont ceux de constructeurs comme Siemens, Xerox, Bosch, Philips, D-Link, Samsung, LG et Belkin). Ils ont découvert **38 vulnérabilités jusqu'alors inconnues impactant 693 firmwares**. En faisant des recoupements, l'équipe d'**Eurecom** parvient à la conclusion que, ensemble, ces vulnérabilités affectent au moins 140 000 appareils accessibles via Internet.

A noter que Linux domine très largement parmi la masse de firmwares réunie par l'équipe d'**Eurecom**. L'OS libre est présent dans 86 % des images analysées (contre 7 % pour les OS propriétaires VxWorks, Nucleus et Windows CE). Mais les chercheurs ont identifié pas moins de 112 versions différentes du système d'exploitation !

Encore et toujours des mots de passe triviaux

Pour leur analyse à grande échelle, les chercheurs ont exploité une architecture de Cloud privé de 90 nœuds. Leur méthode se base sur la découverte d'un certain nombre de failles au sein d'une sélection de firmwares – des vulnérabilités communiquées aux concepteurs des firmwares – puis, via un outil d'analyse de corrélation, à détecter d'autres microcodes sujets aux mêmes faiblesses. Des firmwares entiers ou des composants de ces derniers, développés par des sous-traitants, sont souvent réutilisées par plusieurs constructeurs. Une seule et unique faille est donc susceptible de toucher de nombreux équipements.

Les chercheurs donnent quelques exemples de failles mises au jour (extraction de clefs RSA privées, récupération de mots de passe, backdoors, crédences d'administration codées en dur affectant pas moins de 101 000 appareils…) illustrant les progrès que doivent encore accomplir les constructeurs. Y compris dans des domaines basiques, comme la mise à jour des composants tiers ou les mots de passe administrateurs. Les chercheurs mettent notamment en exergue le stockage de mots de passe hachés, voire en clair, dans des fichiers aux noms trop transparents pour les pirates (*etc/passwd* et*etc/shadow*). « *Ce sont des cibles habituelles pour les assaillants* », notent les auteurs de l'étude. Les mots de passe retrouvés par les chercheurs les plus utilisés sont : le vide, *'pass', 'logout'* ou encore *'helpme'*… Sans commentaires.

Vers des attaques industrialisées

A noter que l'équipe de recherche d'**Eurecom** a packagé sa méthode sous forme deservice Web (encore en bêta) permettant d'analyser les composants d'un firmware.

De façon inquiétante, tant les méthodes qu'exploitent l'équipe de recherche – reposant sur un grand nombre d'automatisations afin de conduire une analyse à grandes échelle – que les pratiques de l'industrie – réutilisation de firmwares entre différents vendeurs, mauvaise gestion des versions de composants – ouvrent la voie à des attaques massivement « industrialisées », susceptibles de compromettre un grand nombre de systèmes. Comme l'illustre le cas récent de vol d'un grand nombre de mots de passe, les cybercriminels semblent déjà avoir compris tous les gains de productivité que ces méthodes sont susceptibles de leur amener.