Une faille critique permet de prendre le contrôle des routeurs, des nas, des systèmes Linux…

Une faille critique permet de prendre le contrôle des routeurs, des nas, des systèmes Linux…

L'éditeur Qualys a mis la main sur une vulnérabilité importante qui permettrait de prendre le contrôle à distance de la plupart des distributions Linux. Les appareils de type routeurs-modems ou NAS sont également concernés.

Les chercheurs en sécurité de la société Qualys ont mis la main sur une faille critique (CVE-2015-0235) qui touche tous les systèmes Linux. Baptisée « Ghost », elle permettrait aux pirates de prendre le contrôle à distance « de tout un système, en se passant totalement des identifiants système », explique l'entreprise dans un communiqué. Un patch a été développé en concertation avec les éditeurs Linux. Il est en cours de diffusion et d'ores et déjà disponible sur certaines distributions, telles de Debian, Red Hat ou Ubuntu.
Cette terrible faille est logée dans une librairie GNU/Linux baptisée« glibc », qui est intégrée dans toutes les distributions Linux et qui permet de gérer les appels système de bas niveau, comme l'allocation d'espace mémoire, l'ouverture de fichiers, etc. Seules les versions antérieures à glibc 2.18 sont vulnérables. « Malheureusement, très de peu distributions Linux ont intégrés les versions récentes de glibc, pour des raisons de compatibilité. C'est pourquoi la plupart sont vulnérables », explique Wolfgang Kandek, directeur technique de Qualys.

Quid des routeurs ou des NAS ?
Comment fonctionne Ghost ? Cette vulnérabilité se caractérise par un dépassement de mémoire tampon (buffer overflow) dans les fonctions gesthostbyname et gethostbyaddr. Ces fonctions sont appelées par les applications Linux quand elles doivent gérer des connexions Internet, comme par exemple les serveurs de messagerie. C'est d'ailleurs la cible sur laquelle se sont penchés les chercheurs de Qualys pour développer un exemple de code d'exploitation : ils ont conçu une attaque dans laquelle il suffit d'envoyer un email vers le serveur pour accéder à l'interface ligne de commande (shell). C'est aussi simple que ça !
Qualys recommande aux administrateurs de mettre à jour leurs systèmes Linux aussi rapidement que possible. Mais une question reste en suspens : quid des nombreux objets connectés que nous possédons tous à la maison, tels que les routeurs-modems ou les disques durs en réseau (NAS) ? « Ils intègrent tous la librairie glibc. Mais pour créer une attaque, il faut également que ces appareils utilisent les fonctions vulnérables. Il faut ensuite trouver le bon vecteur d'attaque. Ce n'est pas évident à priori », souligne Wolfgang Kandek. En somme : pas la peine de paniquer tout de suite. Les pirates vont certainement se pencher sur la question, mais ils vont mettre du temps à développer leurs attaques. Pour réduire le risque, il est conseillé de mettre à jour les firmwares des appareils dès qu'ils seront disponibles.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/643126/ghost-la-faille-critique-qui-permet-de-prendre-le-controle-des-systemes-linux/
Par Gilbert Kallenborn