Stack Clash s'octroie des privilèges sur les systèmes Linux

Plusieurs distributions Linux viennent d'être corrigées. D'autres comme Linux, OpenBSD, NetBSD, FreeBSD et Solaris sur des équipements i386 ou AMD 64 vont très prochainement bénéficier d'une mise à jour pour corriger la vulnérabilité Stack Clash. Laquelle donne la possibilité pour un attaquant de s'octroyer des privilèges en local et d'exécuter du code sur le système racine.

Encore une affaire de mémoire

Cette faille a été découverte par les chercheurs de Qualys et référencée CVE-2017-1000364. Elle se situe dans une pile de gestion de la mémoire des systèmes. L'attaque consiste à contourner les protections introduites dans Linux en 2010 à la suite d'offensives menées en 2005 et 2010 contre cette pile. « *Nos PoC (prototypes, NDLR) augmentent la pile, évitent les protections et s'immiscent dans certaines zones de la mémoire où nous pouvons placer du code à exécuter* », explique Jimmy Graham, expert en sécurité, sur le blog de Qualys. L'équipe a réussi ainsi à créer 7 prototypes d'attaques.

La mémoire dispose d'un mécanisme pour s'agrandir quand un programme a besoin de plus de mémoire. Cet apport est considéré comme une extension de la pile et un attaquant peut écrire du code dessus en supprimant des zones mémoires périphériques ou écrire dans d'autres zones mémoires en supprimant l'extension de la pile.

Protection insuffisante et risque d'exploitation à distance

Pour l'équipe de Qualys, la gravité de cette faille est amplifiée en étant couplée avec d'autres menaces. Elle évoque le cas de Sudo (avec une faille également trouvée par Qualys), une commande qui permet de réaliser des actions avec des droits administrateur. Et ce n'est pas le logiciel de protection de la pile mémoire qui va arrêter ou atténuer le risque. Elle est clairement « *insuffisante* », avoue le spécialiste de Qualys, et peut être contournable notamment grâce à l'extension de pile citée précédemment.

Dans le blog de Qualys, Jimmy Graham n'écarte pas l'hypothèse que la faille Linux soit exploitable à distance à travers des applications spécifiques. « *Nous avons analysé une application (le serveur de messagerie Exim) où nous pensions découvrir cette faille, mais en fait elle n'y était pas.* » Tout en précisant qu'*« il existe des applications pouvant intégrer cette vulnérabilité, mais notre recherche s'est focalisée sur l'élévation de privilèges en local »*. Il est donc urgent d'installer les mises à jour des différentes distributions et systèmes Linux concernés par cette faille.

A lire aussi :

Les serveurs Linux forcés à miner de la crypto-monnaie grâce à Samba

Linux est interdit de Windows 10 S

Code Linux Crédit Photo@isaak55-Shutterstock