Faille zero day : des millions de serveurs Linux et 66 % du parc Android exposés

Depuis de longs mois, une faille permettant une élévation de privilèges traine dans Linux. Dans un billet de blog publié hier, la société de sécurité Perception Point met au jour ce zero day jusqu'alors passé inaperçu et logé dans le noyau Linux depuis sa version 3.8. Soit depuis 2012. La faille, qui permet à un utilisateur ou une application d'accéder à des droits d'accès root, réside dans une fonctionnalité offrant aux applications la capacité de stocker des clefs de chiffrement, des tokens d'authentification ou autres données de sécurité dans le noyau, sous une forme les rendant inaccessibles à d'autres applications. Selon Perception Point, c'est ce trousseau de clefs que des assaillants peuvent détourner, en le forçant à exécuter du code qu'ils injectent. Pour démontrer la réalité de la menace, les chercheurs ont développé un code d'exploit permettant de remplacer un objet stocké via cette fonctionnalité par un code que va exécuter le noyau.

Les implications de ce défaut sont majeures. « *Cette vulnérabilité impacte approximativement des dizaines de millions de PC et serveurs sous Linux (32 et 64 bits, NDLR), et 66 % de l'ensemble de terminaux Android (depuis la version KitKat, NDLR)*, écrit Perception Point dans un billet de blog. *Même si ni nous, ni l'équipe en charge de la sécurité du kernel Linux, n'avons observé d'exploit ciblant cette vulnérabilité, nous recommandons aux équipes de sécurité d'examiner les terminaux potentiellement concernés et de déployer les patchs le plus rapidement possible.* »

Android et Linux embarqués : le casse-tête

Pour les serveurs, les choses devraient aller assez vite : les grands éditeurs de distribution Linux devraient proposer un correctif dans les jours qui viennent. Le déploiement de ces rustines semble en effet s'imposer, la faille mise au jour étant en mesure de donner un accès root à un assaillant parvenant à s'immiscer sur un serveur Linux. Les mesures complémentaires de sécurité (comme le *supervisor mode access prevention* ou le *supervisor mode execution protection*) rendent certes l'exploitation de la vulnérabilité plus complexe, mais ne suffisent pas à l'empêcher totalement.

Pour Android, les choses s'annoncent éminemment plus complexes. Car il n'existe pas de processus de mise à jour bien rodé de l'OS mobile, la plupart des correctifs n'étant pas poussés vers les utilisateurs par les constructeurs de terminaux et les opérateurs. Le cas des Linux embarqués dans divers appareils relève, quant à lui, du casse-tête, les concepteurs de ces appareils n'ayant bien souvent pas prévu de dispositif de mise à jour de l'OS.

Si les cybercriminels et états ont, ces dernières années, avant tout visé Windows, du fait de la taille de son parc installé, ils diversifient aujourd'hui leurs cibles. Le large déploiement de Linux sur les serveurs d'entreprise et la part de marché d'Android dans le mobile en font évidemment des proies intéressantes. Hier, l'éditeur russe d'antivirus Dr Web a ainsi dévoilé l'existence d'un logiciel espion, Linux.Ekocms, qui prend des captures d'écran des postes infectés toutes les 30 secondes avant de les rapatrier sur un serveur. Cette découverte fait suite à la mise au jour d'autres malwares spécialement conçus pour l'OS libre, comme le ransomware Linux.Encoder.

A lire aussi :

Linux progresse de 12,3 % sur le marché EMEA des serveurs

Linux 4.0 inaugure la mise à jour à chaud du noyau

Vente de zero days : une petite entreprise qui ne connaît pas la crise