Une faille de sécurité vieille de 5 ans corrigée dans le noyau Linux

La valeur n'attend pas le nombre des années, se plait à rappeler l'adage, mais en matière de sécurité l'attente est souvent synonyme d'amplification de risques. Les responsables du **Kernel Linux** ont dû méditer sur ces propos en annonçant un correctif sur une **vulnérabilité qui touche le noyau depuis sa version 3.14.3** dans la fonction n_tty_write du fichier *drivers/tty/n_tty.c* du composant *PTY (pseudo terminal) Write Handler.* Concrètement, un attaquant local peut provoquer une corruption de mémoire dans la fonction n_tty_write du noyau Linux, afin de mener un déni de service, et éventuellement d'exécuter du code. Cette faille a été classée sous l'appellation CVE-2014-0196 et un POC (proof of concept) d'une attaque est même disponible.

Si la version 3.14.4 de Linux a été récemment livrée, le 6 mai dernier, la vulnérabilité existerait depuis **plusieurs années** comme le souligne un ingénieur en sécurité de Suse interrogé par *Ars Technica*. *« Cette faille est présente* ***depuis la version 2.6.31 – RC3 du Kernel qui date de 2009.*** » Il n'en demeure pas moins qu'il s'agit d'un problème de sécurité relativement important pour qu'un correctif soit proposé par la communauté Linux. **Plusieurs distributions** sont concernées comme Ubuntu qui vient d'intégrer les corrections. Debian devrait être corrigé prochainement. **Red Hat** de son côté travaille sur la modification de Red Hat Entreprise Linux 6 et Red Hat Enterprise MRG 2, mais indique que RHEL 5 n'est pas concerné par la faille de sécurité.

Ce bug montre la problématique de maintenir à jour et donc de **corriger certains éléments du code** dans les projets Open Source. La faille Heartbleed a montré les limites des tests et de la maintenance du code sur la librairie de chiffrement SSL. La vulnérabilité existait depuis au moins deux ans. Les grands acteurs du web se sont mobilisés financièrement et techniquement pour apporter leur soutien et leur aide aux projets Open Source clés.

Lire également
Près de 320 000 serveurs encore vulnérables à la faille Heartbleed