PMCMA : Un outil OpenSource contre les bugs
Mac et Linux
PostÃ© par : JerryG
PubliÃ©e le : 14/9/2011 15:00:00

La start-up franÃ§aise **Toucan System** vient de publier, sous licence libre Apache 2.0, le code source d'un outil open source prÃ©sentÃ© en avant-premiÃ¨re lors de la derniÃ¨re confÃ©rence Black Hat Ã Las Vegas.

Pour le moins original : pmcma, pour **Post Memory Corruption Memory Analysis**, propose de dÃ©terminer si un bug donnÃ© dans un logiciel est une faille de sÃ©curitÃ©... en tentant de l'exploiter !

Tous les bugs ne sont pas des vulnÃ©rabilitÃ©s : pour se faire, un bug doit prÃ©senter un impact en terme de sÃ©curitÃ© pour le systÃ¨me. La grande majoritÃ© des bugs sur les systÃ¨mes d'exploitation modernes sont de type "Ã©criture invalide en mÃ©moire". Â« *Pmcma est capable de dÃ©terminer si une Ã©criture en mÃ©moire peut Ãªtre transformÃ©e en exÃ©cution de code arbitraire, c'est Ã dire en un Exploit. L'outil est Ã©galement capable de dÃ©terminer le type de faille dÃ©clenchÃ©, ainsi que la probabilitÃ© d'exploitation* Â», dÃ©taille **Jonathan Brossard,** Chercheur en sÃ©curitÃ© Ã©mÃ©rite et co-fondateur de Toucan System.

L'originalitÃ© de l'outil est d'automatiser ces analyses pointues, jusqu'ici rÃ©servÃ©es aux meilleurs spÃ©cialistes du "reverse engineering", via une prouesse technique. **En effet, pmcma, est un dÃ©buggeur d'un type entiÃ¨rement nouveau.** Il permet l'expÃ©rimentation et l'Ã©criture expÃ©rimentale d'exploits, grÃ¢ce Ã une innovation technique de taille : il force le programme analysÃ© Ã se rÃ©pliquer autant de fois que nÃ©cessaire en mÃ©moire pour effectuer une analyse exhaustive, lÃ ou les dÃ©buggeurs classiques ne permettent d'effectuer qu'une seule analyse Ã la fois.

Â« *Cette innovation concerne Ã la fois les dÃ©veloppeurs dÃ©sireux de se concentrer sur les bugs les plus graves d'un point de vue sÃ©curitÃ©, les hackers experts qui vont grÃ¢ce Ã pmcma gagner un temps considÃ©rable en reverse engineering, mais aussi les utilisateurs finaux qui vont dÃ©sormais pouvoir effectuer facilement de bien meilleurs rapports des bugs qu'ils rencontrent, et ainsi permettre aux dÃ©veloppeurs de les corriger en un temps record* Â», explique encore **Nicolas Massaviol**, Directeur technique et co-fondateur de **Toucan System**.

DisponibilitÃ©

L'outil pmcma est disponible gratuitement

PubliÃ© sous la licence libre Apache 2.0.

Il fonctionne actuellement sous les systÃ¨mes d'exploitation GNU/Linux et Android, munis de microprocesseurs Intel 32 ou 64 bits.

Des versions Mac OSX et BSD sont prÃ©vues d'ici la fin de l'annÃ©e.