Le FBI soupçonné d'avoir intégré des backdoors dans OpenBSD

- Informatique - Sécurité Informatique -

Date de mise en ligne : vendredi 17 dÃ©cembre 2010

Spyworld Actu

Un expert employé à la fin des années 90 par le FBI a informé le fondateur de la communauté OpenBSD avoir développé au sein d'une cellule spéciale des portes dérobées. Celles-ci permettraient de dérober des clés de chiffrement et d'intercepter du trafic chiffré. Un audit du code est en cours.

Wikileaks n'a pas le monopole des révélations. Celle qui agite la communauté OpenBSD émane directement de son fondateur Theo de Radt. C'est un message électronique de Gregory Perry, ancien directeur technique de NetSec (devenu Verizon Business Security) qui a mis le feu aux poudres.

Gregory Perry a profité de l'expiration d'une clause de confidentialité signée avec le FBI pour révéler l'affaire. L'expert a ainsi informé Theo de Radt avoir assisté techniquement le FBI à la fin des années 90 dans le but d'insérer du code dans OpenBSD.

Les parefeu et VPN reprenant le code d'OpenBSD potentiellement concernés

Objectif du projet : permettre à l'agence fédérale américaine d'effectuer des interceptions. Les développements de la cellule formée par le FBI portaient en effet sur « des backdoors dans des systèmes de cartes à puce et dans des frameworks cryptographiques » d'OpenBSD analyse LeMagIT.

Pour Gregory Perry, l'existence de ces backdoors justifient notamment l'attachement manifesté par le FBI à promouvoir OpenBSD dans les solutions parefeu et VPN. Depuis les 10 dernières années, le code du système d'exploitation a cependant beaucoup évolué.

Des accusations qui restent à démontrer

Mais Gregory Perry encourage le fondateur de la communauté OpenBSD et ses membres à auditer le code lié à la cryptographie, et en particulier les contributions de Scott Lowe.

Ce dernier, expert de la virtualisation chez EMC, est en effet directement pointé du doigt par Perry qui l'accuse de travailler pour le compte du FBI en promouvant l'utilisation de machines virtuelles OpenBSD dans vSphere de VMware.

Scott Lowe a rapidement réagi sur son blog pour démentir ces informations. Malgré le scepticisme de certains experts à l'égard des différentes accusations formulées par Perry, celles-ci sont malgré tout prises avec sérieux.

Le code source soupçonné d'abriter des portes dérobées ayant été largement réutilisé dans d'autres produits, notamment des distributions, l'affaire dépasse la seule communauté OpenBSD. L'audit du code, et en particulier du stack IPSec, est quoi qu'il en soit lancé.

Post-scriptum :

http://www.zdnet.fr/actualites/le-f...