Vulnérabilité dans le cryptage des disques : « y'a pas le feu au lac »

La publication d'un rapport début 2008, réalisé par des chercheurs de l'Electronic Frontier Foundation (EFF), l'université de Princeton et Wind River Systems, et présentant une vulnérabilité dans les systèmes de cryptage de disques n'inquiète pas spécialement pas les éditeurs…

Chez Microsoft, l'on s'est empressé d'envoyer un porte-parole essuyer le feu de la presse spécialisée. En guise d'interlocuteur, le responsable des produits sécurité de la firme de Redmond, Russ Humphries a pris le ton de la défense estimant que ni les clients grand public, ni les utilisateurs professionnels des solutions de l'éditeur ne devaient s'émouvoir de cette vulnérabilité.

De son côté, le pionnier du cryptage PGP s'est associé à Microsoft afin de minimiser le risque présenté comme important par ledit rapport. PGP. Interrogé par nos confrères de VNUnet.com, il estime *« que les produits PGP ne sont pas concernés pas cette technique, mais que cette dernière est potentiellement réalisable sur tous les disques utilisant des technologies de chiffrement avancées. «*

Enfin, CheckPoint estime que cette attaque de « cool booting » ou à froid, est possible en théorie. Mais très difficile à réaliser dans la réalité. Une affirmation qui a de quoi laisser septique quand on sait que les différentes clés de cryptage peuvent être contournées.

Pour contrer cette attaque, il existe une méthode toute simple, les entreprises doivent déployer un volume virtuel qui n'est monté que lorsqu'il est utilisé et systématiquement fermé après utilisation.

Rappelons que selon les chercheurs à l'origine de cette découverte, un attaquant, particulièrement tenace et rancunier, pourrait retrouver des clés de cryptage en accédant à la mémoire d'une machine récemment éteinte.

Selon le document, même après la fermeture d'un poste, un hacker pourrait extraire la mémoire de la boîte, à partir des éléments stockés sur les chipsets DRam récupérés.