Sécurité : les entreprises négligent les mises à jour Windows

« Cette faille découverte par SkyRecon concerne l'interface WLPCI de Windows (Windows Local Procedure Call Interface). Si elle est exploitée par des cybercriminels, elle peut entraîner des problèmes similaires à ceux provoqués par le ver Sasser dont la première apparition remonte à 2004 » explique Calum MacLeod, directeur européen de Cyber Ark.

D'après lui, les failles permettant l'élévation des privilèges d'un utilisateur ne sont pas nouvelles, en réalité c'est même tout le contraire. Pour le chercheur les premières attaques exploitant ce filon remontent à 1980.

« L'on se souvient notamment d'une fameuse faille de sécurité dans les systèmes DEC 10 au milieu des années 80. Cette dernière permettait aux utilisateurs ou aux programmes de changer d'identité à volonté et ainsi obtenir différents privilèges d'administration » rappelle MacLeod.

« Heureusement pour les managers des systèmes DEC 10 (principalement utilisé dans les écoles), les hackers de l'époque utilisaient principalement cette faille pour utiliser des ressources supplémentaires afin de jouer à des jeux vidéo. Rien de malveillant. »

MacLeod rappelle dans sa note que le problème a été corrigé, mais qu'il existe encore beaucoup d'entreprises qui n'ont pas encore téléchargé ce patch. Il explique qu'il est impératif de se protéger contre cette faille qui peut avoir des conséquences dramatiques.

« Avec cette porte dérobée, les hackers peuvent obtenir assez facilement les mêmes droits que l'administrateur de la plate-forme. Les cybercriminels ont bien changé depuis les années 80, aujourd'hui ils cherchent surtout à faire de l'argent. »