

Ver Conficker : Microsoft publie un patch pour la fonction AutoRun

On le sait, le ver **Conficker/Downadup** qui fait des ravages sur la planète, utilise notamment la fonction AutoRun des clés USB pour pénétrer dans les systèmes. Microsoft a tenté de réagir en conseillant de désactiver manuellement cette fonction. Mais ce conseil est jugé insuffisant dans un avis publié par l'US-CERT (Computer Emergency Readiness Team) notamment pour Windows 2000, XP et Server 2003.

Microsoft s'est donc vu forcé de trouver une autre solution (tout en sachant que la faille exploitée par le ver est corrigée depuis octobre dernier...). L'éditeur a donc développé une rustine spécifique qui corrige le bogue dans la fonction AutoRun. Elle sera diffusée en mode push à travers Windows Update.

« *Ce patch offre un niveau de protection attendu par les utilisateurs* » commente Ben Greenbaum de chez Symantec.

Rappelons que Downadup exploite une vulnérabilité dans le service Serveur de Windows qui permet l'exécution de code à distance si un système affecté recevait une requête RPC (Remote Procedure Call) spécialement conçue.

Selon Panda Labs, au moins **1 PC sur 16 dans le monde est infecté** par ce ver. Selon Qualys, 30% des machines observées sont toujours non patchées et donc vulnérables à la faille. Quant à F-Secure, il estime à 9 millions le nombre de PC touchés (chiffres de fin janvier).