Microsoft corrige 5 groupes de failles, dont 3 sous SP2

Microsoft publie pour ce mois de décembre cinq bulletins de sécurité avertissant de plusieurs failles qui peuvent fragiliser Windows. Elle ne sont pas classées 'critiques' mais simplement 'importantes', ce qui tendrait à rassurer les utilisateurs de PC sous Windows. Sauf qu'en la matière, rien n'est acquis !

Surprise ! Les premières failles concernent **WordPad**, l'application basique de traitement de texte livrée avec Windows. Les versions XP SP2 et Serveur 2003 sont concernées, mais le risque est faible, ce qui n'est pas le cas sur NT 4.0, 2000 et XP SP1. Un hacker peut prendre le contrôle du système attaqué, au travers d'un site Web détourné ou d'un fichier attaché à un e-mail. Le risque est aussi limité en cas d'installation du traitement de texte Microsoft Word. La seconde faille exploite une vulnérabilité dans **HyperTerminal**, sur les mêmes versions de Windows que précédemment. Une saturation de la mémoire dans l'application de communication de Windows permet à l'attaquant de prendre le contrôle du poste, à l'ouverture d'un fichier perverti. Deux failles menacent **Windows NT Server** dans le service du *Dynamic Host Configuration Protocol* (DHCP). La première permet de désactiver le DHCP par une attaque par dénie de service. La seconde affecte l'exécution de code à distance. Plusieurs failles dans **Windows Internet Name Service** menacent Windows NT Server 4.0, 2000 Server et Server 2003, et permettent de prendre le contrôle d'un serveur par l'intermédiaire d'un paquet détourné sur le composant WINS de l'infrastructure réseau. La dernière vague de failles concerne le **noyau Windows et *Windows Local Security Authority Subsystem Service***, et permet à l'attaquant loggé sur le système de modifier ses privilèges jusqu'à obtenir un accès total. Elle affecte Windows NT Server 4.0, 2000, XP et Server 2003. Le prochain bulletin mensuel de Microsoft, le « *Patch Tuesday*« , est annoncé pour le second mardi de janvier.