EEye annonce une vulnérabilité critique sur Windows

Le problème de sécurité, de type «

Buffer overflow», serait situé sur le client SMB, plus particulièrement dans le driver «MRXSMB.SYS» qui est responsable des opérations et réponses SMB. Le protocole SMB (*Server message block*) est utilisé pour le partage de fichiers, d'imprimantes et de ressources entre machines sur un même réseau. L'exploitation n'est pas simple mais elle est tout à fait réaliste. Un faux serveur SMB « émulé » sur le réseau pourrait envoyer un paquet malformé qui aurait pour incidence d'exécuter du code arbitraire sur la machine victime qui le réceptionnerait. Microsoft a développé et offre au public un correctif permettant de protéger les systèmes Windows 2000, XP et 2003 de cette faille. Or, l'OS Microsoft Windows NT4.0 est également vulnérable et Microsoft a décidé de ne fournir le correctif qu'aux clients abonnés au support NT4 payant. Si ce n'est pas votre cas, priez! (*) **pour Vulnerabilite.com**