Et deux petites failles Windows, deux !

Microsoft publie deux nouveaux bulletins de sécurité relatifs à Windows NT, 2000 et XP. Bien que les risques soient modérés, les administrateurs sont invités à installer les correctifs "ad hoc"...

Le premier problème affecte uniquement les différentes versions serveur de Windows 2000 et concerne les stratégies de groupe, non implémentées dans Windows NT ou Windows XP. Windows 2000 propose plusieurs méthodes d'accès en lecture aux paramètres définis pour un groupe et stockés dans le GPO (Group Policy Object). Lorsqu'un utilisateur se connecte sur le domaine, il lit la GPO et applique les paramètres contenus. Windows 2000 offre également une méthode de lecture exclusive, laquelle pourrait permettre à un attaquant de verrouiller les fichiers de la stratégie de groupe. Rassurons toutefois les inquiets : la faille n'est accessible qu'à des personnes disposant d'un identifiant et d'un mot de passe au système elle permet de bloquer les applications liées à la nouvelle stratégie de groupe mis en place par l'attaquant mais pas les paramètres appliqués au préalable il n'est pas non plus possible de changer la stratégie de groupe ou de connaître les identifiants d'autres utilisateurs enfin, notre attaquant a de bonnes chances de se faire repérer. Bref, ce n'est pas "l'attaque de la mort qui tue" !

plus méchant, plus compliqué

La seconde faille affecte les principales versions de Windows NT 4.0, Windows 2000 ainsi que Windows XP Professional et les dégâts potentiels peuvent être plus importants. La vulnérabilité concerne la gestion des buffers en liaison avec le service Multiple UNC Provider (MUP) destiné à aider dans la localisation des ressources réseaux identifiées via UNC (uniform naming convention). Le problème est une non-vérification de l'écriture du second buffer lorsque de l'exécution d'une requête MUP. Cette absence de vérification crée la possibilité d'un dépassement de capacité du buffer et, en conséquence, permet à un attaquant de causer un crash système ou la possibilité de faire fonctionner un code de son choix sur la machine attaquée.
Suite de l' article en lien

Par Stéphane Larcher pour :
Silicon

Par

Publié sur Cafeduweb - Archives le samedi 6 avril 2002
Consultable en ligne : http://archives.cafeduweb.com/lire/1565-deux-petites-failles-windows.html