Microsoft corrige 2 failles critiques. Et… problème

Avec 90 % des PC dans le monde équipé avec le système d'exploitation Windows de Microsoft, les mises à jour publiées par l'éditeur intéressent inévitablement la quasi-totalité des utilisateurs d'ordinateurs PC.

Dans son bulletin de sécurité mensuelle du mois de février, Microsoft a annoncé qu'il corrige deux failles de sécurité critiques qui permettraient à un attaquant extérieur d'utiliser son lecteur mail média ou son navigateur Internet pour prendre le contrôle de l'ordinateur. Windows Media Player est destiné à exécuter des fichiers de musique ou de vidéo. La faille permettrait à un hacker, qui diffuserait un fichier multimédia malicieux, de prendre l'apparence du lecteur afin de lancer d'autres programmes sur l'ordinateur. Concernant certaines versions de Internet Explorer à partir de la version cinq, la faille sur le moteur de rendu graphique corrigée par Microsoft permettrait de prendre le contrôle total du PC via l'exécution de code à distance. Les cinq failles importantes corrigées par le bulletin de sécurité concernent : – une vulnérabilité dans le plug-in Windows Media Player exécutable sur les navigateurs Internet qui n'ont pas leur origine chez Microsoft ; – une vulnérabilité dans TCP/IP qui peut entraîner un déni de service ; – une vulnérabilité dans le service client Web qui peut permettre l'exécution d'un code distant ; – une vulnérabilité dans l'éditeur de méthode d'entrée coréen qui peut aboutir à une élévation des privilèges ; – une vulnérabilité dans PowerPoint 2000 qui peut entraîner une perte d'information. Le bulletin de sécurité de Microsoft pour février 2006 sur TechNet. **Microsoft reconnaît un problème, lors d'une mise à jour**

L'éditeur de Redmond a fait état, juste après la communication de ses correctifs du mois ('patch day'), de problèmes pouvant survenir lors de l'installation/ exécution d'une mise à jour. En pratique, le problème affecte le **correctif MS06-007**, qui résout une vulnérabilité TCP/IP (risque important, mais non critique, d'attaque avec déni de service). IDG News Service confirme que le problème se pose pour toute installation lancée à partir de: Automatic Updates, Windows Update, Windows Server Update services (WSUS) et Systems Management Server 2003, lorsqu'ils sont utilisés avec l'outil d'inventaire ITMU (Inventory Tool for Microsoft Updates). Pour se garantir, les utilisateurs sont invités à **renouveler l'opération de téléchargement** / 'update' -sauf pour ceux qui ont utilisé l'option « Mise à jour automatique » (automatic update), car le correctif du… correctif s'installera tout seul lors de leur prochaine connexion. Pour les autres, précisément ceux qui ont effectué la mise à jour avant 11h30, heure de Paris, il est recommandé de recommencer le téléchargement. _____ (extrait) _____ Bulletin de sécurité Microsoft MS06-007 Une vulnérabilité dans TCP/IP peut provoquer un déni de service (913446) Paru le 14 février 2006 Version : 1.0 Résumé Personnes concernées par ce document : Les clients utilisant Microsoft Windows Type de vulnérabilité : Déni de service Indice de gravité maximal : Important Recommandation : Nos clients doivent installer cette mise à jour dès que possible. Remplacement de mises à jour de sécurité : Le présent bulletin remplace une mise à jour antérieure. La liste complète se trouve dans la section Forum aux questions de ce bulletin.