Deux failles critiques pour Windows

Le bulletin de sécurité de Microsoft du mois de février est plutôt chargé. L'éditeur annonce deux failles critiques pour Windows, fort heureusement corrigées par un patch adéquat.

La première concerne le système ASN.1 de Windows qui pourrait permettre à un individu malintentionné de prendre le contrôle à distance d'un PC. Cette faille de sécurité affecte les systèmes d'exploitation Windows NT 4.0 (SP 6a), 2000, XP et Server 2003. Elle pourrait se révéler très dangereuse en cas d'attaque virale. La faille peut être exploitée a travers tout service ou application utilisant cette librairie, les plus intéressants étant lsass.exe et crypt32.dll. Lsass.exe (Local Security Authority Service) gère les mécanismes de sécurité de Windows. Il crée le process chargé d'authentifier les utilisateurs pour le service Winlogon. Plus concrètement, cette vulnérabilité peut être exploitée en attaquant tout service utilisant des certificats comme par exemple un serveur web encapsulé dans du ssl, un e-mail ou un ActiveX signé digitalement. Le service Kerberos est aussi vulnérable ainsi que toute application utilisant NTLMSSP authentification. D'après Marc Maiffret de Eeye Digital, la compagnie qui a découvert cette vulnérabilité : *« Si vous utilisez Windows NT 4.0, Windows 2000, Windows XP, ou Windows 2003, vous êtes vulnérable a 99.9999% sans même prendre en considération votre configuration »*. La deuxième faille fragilise le service WINS (Windows Internet Naming Service). En envoyant une série de paquets malformés, il est possible qu'un pirate ou 'hacker' puisse provoquer, à distance, l'arrêt du service WINS. Et, sous certaines conditions, il pourrait même exécuter des commandes arbitraires. Le déni de service qui touche WINS sur plate-forme Windows 2003 Server serait dû à un dispositif de sécurité interne à Microsoft Windows: ce dernier bloque prématurément ce module de nommage lorsque des paquets corrompus sont détectés par le système. Sur les plates-formes NT et Windows 2000, les effets sont différents. Là, le service WINS rejette tout simplement les paquets malformés et donc il n'est pas possible de provoquer une attaque par déni de service ni d'exécuter du code arbitraire. Par souci de sécurité Microsoft offre tout de même un correctif pour ces plates-formes tout en se préoccupant de savoir si une méthode pour exploiter la faille sur ces versions antérieures des serveurs pourrait être mise au point… Selon notre partenaire « isecurelabs.com », ce problème de sécurité a été jugé « sérieux » par Microsoft. Il a été découvert par la société Qualys, qui propose une solution d'audit de vulnérabilités en mode ASP. Les patchs sont disponibles sur le site de Microsoft. **Olivier Devaux**, Vulnerabilite.com (c)