20 failles à corriger: le serveur de Microsoft sature!

C'est l'une des plus importantes mises à jour que Microsoft ait jamais mis en ligne, avec pas moins de 20 failles corrigées. La majorité des défauts reconnus sur Windows NT Workstation et Server, Windows 98, Windows XP, Windows 2000 et Windows Server 2003 ne sont pas considérés comme sérieux, mais d'autres sont déclarés critiques.

Fidèle à sa politique inaugurée voici quelques mois, Microsoft a décidé de ne proposer qu'une mise à jour mensuelle à l'aide d'un unique patch qui fixe l'ensemble des failles. Patch unique mais proposé en quatre versions afin de s'adapter aux OS. Les systèmes d'exploitation de Microsoft corrigés sont les suivants : Microsoft Windows 2000 Advanced Server Microsoft Windows 2000 Datacenter Server Microsoft Windows 2000 Professional Microsoft Windows 2000 Server Microsoft Windows NT 4.0 Server Microsoft Windows NT 4.0 Server Terminal Server Edition Microsoft Windows NT 4.0 Workstation Microsoft Windows Server 2003 Datacenter Edition Microsoft Windows Server 2003 Enterprise Edition Microsoft Windows Server 2003 Standard Edition Microsoft Windows Server 2003 Web Edition Microsoft Windows XP Home Edition Microsoft Windows XP Professional Les 14 principales failles corrigées sont les suivantes : 1) Une erreur binaire dans LSASS (*Local Security Authority Subsystem Service*) sous Windows 2000 et Windows XP, qui peut entraîner une surcharge mémoire via un message détourné qui permet d'exécuter un code arbitraire pour contourner les privilèges systèmes. 2) Une erreur binaire dans LSASS (*Local Security Authority Subsystem Service*) sur une requête LDAP sous le contrôleur de domaine de Windows 2000, qui permet de rebooter le domaine vulnérable par l'intermédiaire de la requête. 3) Une erreur binaire sur la librairie Microsoft SSL (*Secure Sockets Layer*), qui permet l'exécution d'un code arbitraire par l'exploitation par une surcharge mémoire via un message PCT (*Private Communications Transport*) détourné. 4) Une erreur binaire dans le Winlogon (*Windows logon process*) sur Windows NT 4.0, Windows 2000, et Windows XP membres d'un domaine, qui permet de modifier l'objet de ce dernier afin d'entraîner une surcharge mémoire. 5) Une erreur binaire dans le rendu de Metafiles peut être exploitée afin d'entraîner une surcharge mémoire via des fichiers spécialement modifiés. 6) Une erreur de validation des entrées dans '*Help and Support Center*' lors de la saisie d'une URL HCP peut être exploitée pour exécuter un code arbitraire sur un système vulnérable par l'intermédiaire de URL HCP détournée. 7) Une erreur dans Utility Manager lors du lancement d'une application peut être exploitée par un utilisateur local pour modifier ses privilèges sur Windows 2000. 8) Une erreur dans le gestionnaire de tâches de Windows XP permet dans certaines circonstances de créer des tâches qui seront exécutées avec les privilèges SYSTEM. 9) Une erreur sur une interface programmée pour la création d'entrées dans une LDT (*Local Descriptor Table*) peut permettre d'accéder à la mémoire protégée afin de modifier les privilèges. 10) Une erreur binaire dans l'implémentation du protocole H.323 permet d'entraîner une surcharge mémoire via une requête H.323 spécialement modifiée. 11) Une erreur dans le sous système VDM (*Virtual DOS Machine*), un composant du système d'exploitation, peut être exploitée afin d'accéder au noyau protégé de la mémoire afin de modifier les privilèges. 12) Une erreur binaire dans l'interface Negociate SSP (*Security Software Provider*) peut entraîner une surcharge mémoire via un message réseau détourné, ce qui en cas de succès peut aboutir à un dénie de service. 13) Une erreur sur la librairie Microsoft

SSL (*Secure Sockets Layer*) lors de la réception d'un message SSL peut être exploitée afin de bloquer l'acceptation des connexions SSL, voir de redémarrer. 14) Une erreur '*double free*' dans Microsoft ASN.1 Library peut être exploitée pour corrompre la mémoire et entraîner un dénie de service par l'exécution d'un code arbitraire. **Les patchs sont disponibles sur les sites de Microsoft**. Mais attention, l'importance de cette mise à jour massive a provoqué la saturation du site « Windows Update » qui était par moment injoignable ce mercredi. Les utilisateurs inquiets devront patienter avant d'être rassurés…