

Nouvelle salve de failles dans Windows

Outre la mise à jour mensuelle de Microsoft, qui vient corriger de nombreuses failles sur Internet Explorer (

lire notre article), les clients de Windows iront faire leur marché pour corriger de nombreuses autres failles également corrigées par l'éditeur: – Un lot important de modules ou systèmes Windows fragilisés par des failles jugées très critiques : Windows Server 2003 Standard, Enterprise et Datacenter Edition, Windows NT 4.0 Server, Terminal Server Edition, Windows Millenium, Windows 98 et Second Edition, Windows 2000 Server, Professional, Datacenter Server et Advanced Server, Windows Server 2003 Web Edition, Windows XP Home Edition et XP Professional. Tous ces systèmes présentent des failles récurrentes, sur des fonctions oubliées sous Window Management API, sur une erreur de référentiel mémoire sous VDM (*Virtual DOS Machine*), sur une erreur sous Graphics Rendering Engine avec les fichiers WMF (Windows Metafile) et EMF (Enhanced Metafile), et sur la structure de données CPU du Windows Kernel. – Windows présente une faille liée au protocole NNTP (*Network News Transfer Protocol*). L'exécution d'un code arbitraire peut entraîner une saturation de la mémoire (*buffer overflow*). La faille ne touche pas les environnements Exchange Server 2002 et 2003. – Risque de déni de service et d'exposition d'informations sensible sous Windows NT avec un défaut détecté sur RPC Runtime Library. – Et une faille sous XML ! Encore un risque de déni de service, sous WebDAV XML Message Handler cette fois, Si le nombre des attributs est trop important. Le SP2 corrige la faille. – Idem pour la vulnérabilité, avec risque de « buffer overflow », rencontrée sur le service NetDDE. – Le tableur Excel présente une faille accessible via des fichiers exportés qui peuvent compromettre le système utilisateur. – Reliquat de la faille sur le format JPEG, lire nos articles, les 'viewer' de PowerPoint et de Visio 2002 et 2003 sont mis à jour. La faille est jugée critique. – Les fichiers 'zip' compressés ne sont pas oubliés, avec le risque de « buffer overflow » sur les 'Compressed Folders'. – Et un autre risque de « buffer overflow » sur un composant SMTP sur des réponses DNS sous le rarissime Windows XP 64-Bit Edition Version 2003. Cette longue liste ne semble pas close pour ce mois-ci, à suivre ! **Patches et mises à jour s'imposent sur le site de Microsoft.**