Patch day: Microsoft publie 10 correctifs

Le deux derniers bulletins de sécurité mensuel de l'éditeur avaient laissé sur leur fin. Une seule faille corrigée en mai, aucune en mars: on attendait Microsoft au tournant.

Le patch day de juin est autrement plus fourni! L'éditeur a mis en ligne dix rustines dont trois corrigent des failles jugées critiques. Commençons donc par celles-ci. -Internet Explorer (5.01 SP1&2, 5.5 pour Me et 6.0) Plusieurs vulnérabilités peuvent permettre à un attaquant de prendre le contrôle intégral d'un système affecté via l'exécution de code à distance. Les problèmes concernent la gestion d'images PNG spécialement conçues, et la gestion de certaines requêtes d'affichage de contenu XML. -Windows (98, Me, 2000, XP, Server) Il existe dans HTML Help des vulnérabilités qui peuvent permettre à un attaquant de prendre le contrôle intégral d'un système affecté. -Windows (2000, XP, Server 2003) Une vulnérabilité dans SMB (Server Message Block) peut permettre à un attaquant de prendre le contrôle intégral d'un système affecté. Un attaquant doit d'abord s'authentifier avant de pouvoir exploiter cette vulnérabilité. Failles « importantes »: -Windows (XP, Server 2003) Web Client Il existe dans le service WebClient une vulnérabilité qui peut permettre à un attaquant de prendre le contrôle intégral d'un système affecté. Pour exploiter cette vulnérabilité, l'attaquant doit disposer d'informations d'identification valides pour ouvrir une session en local. -Exchange Server 5.5 Outlook Web Access Vulnérabilité de transfert de script entre sites qui peut permettre à un attaquant d'exécuter un script malveillant dans Outlook Web Access. -Outlook Express 5.5 & 6 Il existe une vulnérabilité qui peut permettre à un attaquant de prendre le contrôle intégral d'un système affecté. L'intervention d'un utilisateur est nécessaire pour exploiter cette vulnérabilité ; l'attaquant doit également persuader l'utilisateur de se connecter à son serveur News (NNTP, Network News Transfer Protocol). -Windows Interactive Training Faille qui permet à un attaquant de prendre le contrôle intégral d'un système affecté. Par défaut, Microsoft Windows Interactive Training n'est pas installé. Failles « modérées » Elles concernent Microsoft Agent, le client Telnet et Microsoft ISA Server.