

'Tuesday patches' de Microsoft: correctifs sur serveur DNS, Office et Exchange

La livraison de correctifs par Microsoft pour ce « path tuesday » est copieuse. Toutes les mises à jour ne sont cependant pas critiques. Deux sont particulièrement à surveiller: les patches MS07-026 et MS07-029 qui concernent des failles dans le serveur de messagerie Exchange et dans le serveur de noms de domaine, ou serveur DNS (*domain name server*).

Les 19 patches de ce 8 mai ont été rangés en sept groupes de correctifs ou mises à jour ('updates'). Microsoft considère ces 7 'upgrades' comme « critiques ». En réalité, deux correctifs seraient particulièrement urgents à apporter: les 'patches' MS07-026 et MS07-029 qui corrigent des failles dans Exchange et dans le serveur de noms de domaine, Windows DNS server.

La faille dans **Exchange**, très récemment mise à jour, pourrait permettre à un pirate de prendre le contrôle de tout un serveur de messagerie.

Si un hacker malveillant parvenait à développer le code « exploit » adéquat, il pourrait installer des logiciels pirates sur le serveur à partir d'un simple e-mail – ce qui serait ensuite très difficile à bloquer.

La faille dans le **serveur DNS** est, elle, identifiée depuis plus d'un mois. On sait que des codes « exploits » ont déjà été développés et certains éditeurs de logiciels en sécurité ont signalé des attaques en ligne qui s'y réfèrent.

Cette faille qui concerne Windows 2000 et Windows Server 2003, consiste à envoyer des paquets RPC pirates (remote procedure call, ou requête de procédure à distance), pour accéder à des fonctions ou commandes du serveur DNS.

Les autres correctifs concernent, pour l'essentiel, **Internet Explorer** et Office (**Excel** et **Word**) ainsi que le logiciel d'encryptage **Capicom**, utilisé dans le serveur BizTalk.