Une faille critique corrigée dans Thunderbird

La fondation **Mozilla** a récemment mis à jour son outil de courrier électronique, **Thunderbird**. La mouture **2.0.0.23** corrige une vulnérabilité classée comme étant critique. La mise à jour du logiciel est donc vivement recommandée. Elle sera automatique dans la plupart des cas, même s'il est ici conseillé de l'effectuer manuellement, en téléchargeant directement l'application sur le site du projet.

La faille a été découverte par **Dan Kaminsky** et touche les communications chiffrées. Un bogue permet d'utiliser des certificats créés par des pirates sur n'importe quel site, et ainsi de rendre caduc tout système de chiffrement des communications.

Cette faille touche à la fois Firefox 3.0, SeaMonkey et Thunderbird. Avec ce dernier, l'impact de la vulnérabilité restera assez faible, les communications chiffrées n'étant pas communes dans les flux de ce type. Elle pourra toutefois être utilisée pour exécuter du code distant sur la machine de l'utilisateur, **en corrompant le système de mise à jour intégré au logiciel**, comme l'a signalé l'expert indépendant **Moxie Marlinspike**.

Notez que Firefox 3.0.13 corrige cette faille. Contrairement à ce qui a pu être écrit ici et là, Firefox 3.5 n'est pas concerné par ce problème. Enfin, pour SeaMonkey, il faudra attendre la sortie de la mouture 1.1.18, prévue prochainement.