Avec Mac OS X 10.3, Apple corrige 3 failles et 13 bugs!

Prendre le contrôle d'un Mac sous OS X, c'est ce qu'autorisent les trois failles de sécurité découvertes par @Stake dans les précédentes versions du système d'exploitation d'Apple. Les **trois failles** concernent le noyau du système! A l'installation d'une application, tout d'abord, une personne malveillante peut usurper des privilèges d'accès au système, dont le module d'authentification / autorisation semble peu sûr! La création, autorisée par le système, d'un fichier d'identification des utilisateurs, avec en particulier leur mot de passe, est la seconde faille. Elle est recherchée par les 'hackers', car elle permet d'accéder à des informations théoriquement réservées. Enfin, la saisie d'une longue ligne de commandes peut entraîner un risque de dépassement de mémoire tampon (*buffer overflow*), avec, pour conséquence, de bloquer le système et de lancer un redémarrage. Une faille bien pratique pour exécuter un code de prise de contrôle du Mac. **13 'bugs' selon Secunia** Pour Secunia, autre spécialiste de la sécurité en environnement Apple, ce serait pas moins de 13 bugs qui seraient corrigés par la mise à niveau sous OS X 10.3. Ces vulnérabilités concernent en particulier des problèmes NFS et de temporisation TCP, des erreurs 'bornées', une vulnérabilité dans Open SSH, une possibilité d'attaque en liaison synchrone, etc. En l'absence de mise à jour, @Stake et Secunia conseillent de passer à la nouvelle version d'OS X 10.3, qui ne présente plus ces failles.