Failles critiques dans Mozilla et Linux

Secunia nous informe de la découverte de failles de sécurité critiques dans Mozilla, Mozilla Firefox et Mozilla Thunderbird, qui proviennent de la librairie 'libpng', la même qui menace les environnements Linux.

Les failles proviennent d'erreurs dans le pointeur NULL lors du traitement de fichiers PNG, et peuvent aussi être exploitées via des sites Web détournés ou des e-mails sous des applications en liens avec 'libpng'. Exploitées par des personnes mal intentionnées, ces failles permettent de compromettre un système vulnérable ou d'entraîner un déni de service. Avec en prime pour Linux le risque de saturation de la mémoire (*buffer overflow*). Vulnérabilité.com nous confirme qu'il serait « *possible de fabriquer une image au format PNG qui lorsqu'elle serait visualisée avec l'un de ces butineurs forcerait celui-ci à exécuter du code arbitraire ou causer un déni de service (crash du butineur). D'une manière générale, la quasi-totalité des logiciels qui utilisent les versions de la libpng vulnérables est affectée*« . Les failles sous Mozilla ont été corrigées à partir des versions Mozilla 1.7.2, Firefox 0.9.3 et Thunderbird 0.7.3. Concernant les distributions de Linux, il convient de se tourner vers leurs distributeurs. Plusieurs d'entre eux ont déjà annoncé la mise à jour de leur distribution : Mandrake, Debian, Fedora, Red Hat, SuSE, Gentoo.