Date: Mardi 13 septembre 2005 à 19:36:32
Sujet: 3 Sécurité et Hacking

Faille critique dans Mozilla Firefox et Netscape

Une faille extrémement critique vient d'être découverte (le 09/09/2005) dans Mozilla Firefox, Mozilla Suite et Netscape. Elle permet grace a une page HTML astucieuse de prendre le controle a distance d'un système vulnérable en causant un déni de service.

Description de la faille :
Cette faille, de type buffer overflow (dépassement de mémoire tampon) exploite les défaillances de la fonction NormalizeIDN qui permet habituelement la normalisation de certains jeux de caractéres locaux mais qui est pourvue d'une mauvaise gestion de certains tags HTML contenant des URLs malformées contenant le caractère 0xAD.

Versions touchées :
Cette faille touche de nombreuses versions de Mozilla Firefox, les versions 1.0.6 et inférieures sont infectées ainsi que la nouvelle version 1.5 bêta 1. Cette faille affecte également Mozilla Suite 1.7.11 et inférieures ainsi que Netscape 8.0.3.3 et inférieures. Correctif et Protection :
Aucun correctif n'a encore été élaboré, et seul un patch temporaire désactivant la fonction IDN mise en cause a été mis au point par la Fondation Mozilla.
Pour parer à toutes attaques éventuelles, vous pouvez vous même désactiver cette fonction.
Pour cela, il suffit d'ouvrir Mozilla Firefox, d'entrer about:config dans la barre d'adresse, d'appuyer sur la touche Entrée.
Cherchez ensuite dans la fenetre qui s'ouvrira la ligne network.enableIDN, et mettez sa valeur à False (si ce n'est déja fait) en double-cliquant sur cette ligne.
La valeur devrait changer et votre systéme sera dès lors protégé des attaques exploitant cette faille.