Face au Javascript, Firefox 2.0 risque de planter

La vulnérabilité n'est pas l'apanage de Microsoft. La Fondation Mozilla, qui est à l'origine du développement du navigateur alternatif vient de confirmer la découverte faite par l'un des ses contributeurs, un défaut dans la nouvelle mouture du programme l'empêcherait de prendre en charge certains éléments écrits en Java script dans une page Web.

Cette faille d'une dangerosité moyenne reste problématique dans la mesure où elle peut entraîner le crash du navigateur après le lancement par un garnement de la toile d'une attaque par DOS (déni de service).

Pour l'instant, ce bug ne semble pas inquiéter outre mesure la Fondation Mozilla qui estime que ce problème est certes ennuyeux, car il provoque le plantage du navigateur, mais qu'il n'est pas vraiment dangereux.

Reste que le plantage du navigateur n'est pas du meilleur effet, cependant c'est l'unique menace qui pèse sur les utilisateurs du fameux panda rouge. Un porte-parole de la Fondation a déclaré que cette faille ne pouvait pas être exploitée par d'autres codes arbitraires.

Les internautes sont prévenus, si une page web contenant du javascript entraîne la fermeture du navigateur il ne servira à rien de sauter au plafond, seulement de signaler l'URL en question à Mozilla et de relancer le programme. Ce bug a été repéré par BugTraq dès le lancement du navigateur, mais il aura fallu une semaine pour attendre le verdict de Firefox.

De son coté IE7 est victime d'une faille qui l'expose à l'hameçonnage (phishing). Rappelons que le 19 octobre, le site internet Secunia a annoncé avoir repéré une première faille dans le navigateur de Microsoft.

De son côté, le géant américain explique que cette faille est liée à Outlook Express mais pas à IE7 ; plus spécifiquement à la DLL inetcomm.dll qui n'est pas installée, ni mise à jour par IE7.

Les jours passent…Puis Secunia revient à la charge avec la découverte d'une nouvelle faille moins critique dans IE7, cette dernière pourrait permettre des attaques par phishing via la bonne vieille technique du spoofing d'URL.

Comme pour les conflits armés, en informatique le risque zéro n'existe pas. La sortie de ces deux nouvelles versions met également en exergue une véritable course entre les chasseurs de bugs. Mais par chance, les failles trouvées à ce jour ne mettent pas véritablement les données des internautes en péril. Pour l'instant.