Une faille critique pour Firefox 3.5 !

Le nouveau moteur JavaScript TraceMonkey intégré à **Firefox 3.5** aura été la source de bien des soucis. Des problèmes liés à sa mise au point ont retardé la sortie de ce navigateur web, qui s'est fait ainsi griller la politesse par Google Chrome 2.0 et Apple Safari 4.

Pire, lors de la sortie de Firefox 3.5, nous avons pu constater que TraceMonkey n'arrivait pas à la hauteur de ces deux concurrents et qu'il provoquait même des microcoupures très désagréables dans le fonctionnement du logiciel.

En épilogue à ce triste épisode, une faille critique a été découverte dans TraceMonkey. Celle-ci permet d'exécuter du code sur la machine de l'utilisateur hôte, et donc d'en prendre le contrôle à distance. Un des bogues relevés dès le lancement de Firefox 3.5 est à la source de cette vulnérabilité, qui a été confirmée officiellement hier sur un des blogues de la fondation Mozilla.

Quand l'irresponsabilité entre en jeux

En général, ce genre de faille est classé comme étant « critique ». Hélas, Simon Berry-Byrne fournit un *exploit* permettant de la mettre en œuvre. Il ne fonctionne aujourd'hui que sous Windows, mais son **adaptation aux autres systèmes d'exploitation semble plutôt aisée.**

Les règles en vigueur dans le **monde de la sécurité suggèrent que les *exploits* ne soient jamais rendus publics,** tant que les développeurs du logiciel touché n'ont pas eu le temps de proposer un correctif.

Nous ne pouvons donc que nous indigner de ce procédé qui met cette vulnérabilité à la portée des *script kiddies*, une population de bricoleurs écervelés, toujours prompts à prendre le contrôle de vastes parcs de machines dans le seul but de faire la preuve de leur « savoir-faire »… dans le domaine du copier/coller de code (*sic.*).

En souhaitant profiter d'une éphémère célébrité, Simon Berry-Byrn, use donc d'un procédé plus que critiquable. Les responsables de la **fondation Mozilla sont ainsi contraints de précipiter la sortie de Firefox 3.5.1** (initialement prévue pour la fin de ce mois), au risque de laisser passer de grossiers bogues. Dans l'attente, ils proposent une rustine temporaire pour pallier cette fuite d'informations prématurée.

Une seule solution : basculer de TraceMonkey vers SpiderMonkey

Voici le détail de la manipulation permettant de combler cette faille : dans la barre de navigation du logiciel, saisissez *« about:config »*. Passez la mise en garde de sécurité, puis filtrez la liste en choisissant le terme *« jit »*. Double cliquez enfin sur la ligne *« javascript.options.jit.content »* pour passer sa valeur à *« false »* et redémarrez le navigateur.

Grâce à cette manipulation, **Firefox 3.5 utilisera le classique moteur JavaScript SpiderMonkey**, qui n'est pas touché par cette faille, mais qui se montre – malheureusement – bien plus lent que TraceMonkey. Notez qu'il faudra effectuer l'opération en sens inverse une fois que vous aurez installé la mise à jour (future) qui corrigera cette vulnérabilité.

Si cette manipulation vous semble trop complexe, lancez le logiciel en*« mode sans échec »*. Vous ne pourrez alors plus utiliser les modules complémentaires, mais **TraceMonkey sera automatiquement désactivé.**