Juillet noir pour les navigateurs Internet

Tout a commencé alors que H.D Moore développait un outil ? baptisé hamachi ? lui permettant d'automatiser la détection de vulnérabilités localisées dans des Contrôles ActiveX.

La technique que H.D Moore souhaite mettre en ?uvre avec ce logiciel est la méthode dite du « fuzzing ». Ce procédé peut être apparenté au « brute forcing ». Il s'agit d'envoyer des données aléatoires et aléatoirement aux différents points d'entrée de l'ActiveX et d'observer ses réactions.

En cas de « crash » du navigateur ou de comportements anormaux, il y a de fortes chances pour qu'une faille ne soit pas très loin ? La technique du fuzzing est également utilisée pour dénicher des vulnérabilités de type « buffer overflow » lorsqu'on ne dispose pas du code source d'un binaire. C'est également grâce à cette méthode que la vulnérabilité ASN.1 fut découverte.

Après plusieurs semaines de tests intensifs, les résultats tombent et les failles pleuvent. Grâce à son outil et à d'autres programmes du même genre (axfuzz, COMRaider, DOM-Hanoi, CSS-Die, MangleMe), H.D Moore a découvert de nombreux défauts dans les navigateurs Internet Explorer, Firefox, Safari, Konqueror et Opera. Tous les jours du mois de juillet, une vulnérabilité sera postée sur un blog dédié et ironiquement intitulé BrowserFun.

Nul doute que la sécurité des navigateurs deviendra un véritable enjeu dans les prochains mois. La fondation Mozilla en fait d'ailleurs un argument de poids pour Firefox et aux vues des parts de marchés gagnées ces derniers mois, il semble bien fonctionner. Moralité : en juillet, surfez patché … autant que vous le pouvez !