Firefox faillible, la librairie GIF en cause

La vulnérabilité, de type « heap overflow » (de la famille des buffer overflow), affecte la librairie chargée du traitement des images au format GIF.

L'exploitation de cette faille, à travers la visualisation d'une image GIF piégée, pourrait permettre l'exécution de code arbitraire avec les privilèges de l'utilisateur utilisant Firefox. Toutes les versions antérieures à Firefox 1.0.2 sont vulnérables. Il est conseillé de mettre à jour votre navigateur. Pour information, la librairie a également été corrigée dans les logiciels Thunderbird et Mozilla Suite. Une fois de plus, c'est une librairie de traitement d'images qui se révèle être le maillon faible. Par le passé, plusieurs produits tournant sur plates-formes Microsoft Windows et Linux ont vu leur sécurité mise en péril par les librairies de traitement des images JPEG, BMP et même PNG. On se rappelle de la fameuse faille dite « JPEG GDI+ » qui fut massivement exploitée par les pirates en septembre 2004. Heureusement, en ce qui concerne cette faille sur Firefox, la réactivité de la communauté open source a permis de réduire la fenêtre d'exposition aux risques en publiant rapidement un correctif. (*) **pour Vulnerabilite.com**