Le greffon Java ne serait toujours pas sécurisé

Vendredi dernier, nous apprenions qu'une faille critique 0-day touchait le greffon **Java** dédié aux navigateurs web. Une fois n'est pas coutume (mais nous espérons que cela le deviendra), **Oracle** a réagi sans délai et proposé, via **Java SE 7u11** un correctif éliminant ce problème.

Les autorités américaines ne semblent toutefois pas rassurées. L'US-CERT continue ainsi d'alerter les utilisateurs : *« Sauf si vous devez absolument exécuter des applications Java dans les navigateurs web, désactivez le greffon, même après la mise à jour 7u11. Cela contribuera à atténuer les autres vulnérabilités Java qui pourront être découvertes à l'avenir. »*

Fausse alerte ?

Certes, réduire la surface d'attaque de son système est un bon conseil, mais cela est vrai pour tous les logiciels. Crier au loup de la sorte n'est donc pas très 'fair play' envers Oracle, qui a pourtant été exemplaire sur ce cas.

Depuis cette annonce, de nombreux experts en sécurité ont à leur tour jeté de l'huile sur le feu, arguant que le code de Java n'était pas sûr et qu'il serait de toute façon toujours sujet à des failles critiques. L'argument est facile, car c'est le cas de tout logiciel un tant soit peu populaire.

Nous nous inscrivons pour notre part en faux avec cette affirmation. De fait, Adobe l'a démontré : sécuriser un greffon n'est pas une tâche impossible, justement car sa zone de contact avec l'OS reste limitée. Il suffit pour cela de l'intégrer au sein d'un bac à sable (ou de celui des navigateurs, lorsque disponible). Oracle pourrait tout à fait adopter une telle stratégie dans le futur.

Voir aussi
Quiz Silicon.fr – Connaissez-vous les secrets de Java ?