# Faille Firefox, plus de peur que de mal ?

La nouvelle faille découverte ce 17 ou 18 mai par le site Securityview est présentée comme un « déni de service » affectant le navigateur vedette Firefox. Un Proof-Of-Concept (PoC) a été développé et distribué à la communauté. Il s'agit d'un code Javascript placé dans une page HTML qui, lorsqu'elle est interprétée par le butineur, déclenche l'ouverture du client de messagerie e-mail de la victime.

Jusque-là, rien de dangereux direz-vous ? Sauf que si la commande permettant l'ouverture du client de messagerie (Outlook, Thunderbird par exemple) est placée dans une boucle qui va exécuter la même opération plusieurs centaines de fois, la machine de la victime s'écroule et le redémarrage devient nécessaire pour retrouver l'usage de l'ordinateur. Ce qu'on peut appeler un « déni de service ». Cette fameuse commande permettant l'ouverture du client de messagerie est en fait un lien « MAILTO » encapsulé dans un tag HTML « IMG SRC ». Rien de très sorcier donc, si ce n'est que cette commande ne nécessite aucune interaction (donc aucun clic) avec l'utilisateur pour être exécutée. Là est le danger. Chacun connaît par c?ur les fondamentaux de la sécurité informatique qui sont -répétons-le pour les deux du fond qui ne suivent pas… -, l'intégrité, la confidentialité et la disponibilité. Dans le cas qui nous intéresse, seule la disponibilité de la machine est remise en question par cette faille. Tant que la confidentialité ou l'intégrité des données ne sont pas mises en péril, on ne peut pas encore considérer cette faille comme critique. Pourtant, l'heure n'est pas aux réjouissances ni au soulagement. Si aujourd'hui cette vulnérabilité n'est pas si dangereuse que la presse pourrait le clamer, il est toujours temps demain de trouver un moyen de l'exploiter afin d'exécuter des commandes arbitraires sur la machine de la victime. Les chercheurs planchent déjà sur le sujet … Pour le moment, Mozilla n'a pas diffusé d'alerte pour cette pseudo-faille. Seule option pour les internautes qui souhaitent s'en protéger : désactiver Javascript et/ou le lien « mailto ». _____ ***Mise à jour au 22/05/2006*** Internet Explorer semble également touché par le même problème très exactement. Reste à définir quelles versions sont concernées. Merci à Mimah pour l'information.