

Alerte : une faille hautement critique plombe Firefox 2.0

Cette porte dérobée permettrait à un attaquant distant de pénétrer dans le système de l'utilisateur à son insu. Elle concerne la façon dont le navigateur gère les informations URI d'une page Web.

L'URI pour 'Identifiant Uniforme de Ressource', est une chaîne de caractères identifiant une ressource Web physique ou abstraite, et dont la syntaxe respecte une norme mise en place pour le World Wide Web. L'URI, dont l'URL est certainement l'exemple le plus connu permet d'identifier une ressource, mais aussi et surtout dans le cas du jour, d'agir sur elle.

Le problème vient du fait que Firefox lorsqu'il s'installe enregistre dans le registre Windows l'URI « Firefoxurl:// ». Cet « identifiant » est ensuite appelé lors de l'ouverture de l'application et contient les informations personnalisées par l'utilisateur.

Selon [Secunia](#), c'est à ce niveau qu'il y a un problème puisqu'un attaquant pourrait utiliser cet URI pour y glisser un code malveillant utilisant du Javascript.

Ce code serait alors capable de renvoyer l'utilisateur vers une URL mais en utilisant un autre navigateur par exemple Internet Explorer ou Opera. Signalons que Firefox doit être installé pour que l'attaque fonctionne.

Secunia recommande de ne pas installer l'extension chrome. La vulnérabilité est confirmée dans Firefox 2.0.0.4 sur un OS XP SP2 à jour.

D'autres versions sont certainement vulnérables, précise l'éditeur qui recommande, de ne pas visiter de pages Web inconnues et de fermer le gestionnaire des URI. Pour l'instant aucun correctif n'est disponible...