Firefox est victime d'une vulnérabilité « Directory Traversal »

L'information a été confirmée par le responsable de la sécurité du navigateur, Window Synder. Selon la Fondation Mozilla, cette vulnérabilité permettrait à des hackers de dérober des informations personnelles.

La découverte de cette faille est à mettre au profit du chercheur Gerry Eisenhaur. Il a d'ailleurs publié la proof of concept (POC) de sa découverte sur son site Web. Selon lui, le bug réside dans le protocole chrome du panda rouge, chrome étant le moteur en charge de l'interface utilisateur. Il permet à un attaquant de détecter les programmes et les fichiers présents sur un poste. Une fois ces informations récupérées il peut lancer des attaques encore plus malveillantes.

D'après Eisenhaur, un attaquant peut par exemple accéder au fichier de configuration d'un client mail. Mais une condition est nécessaire pour que cette visite impromptue se déroule correctement, l'utilisateur doit avoir installé une extension qui ne s'affiche pas sous la forme d'un fichier compressé .jar.

Les utilisateurs qui sont menacés sont uniquement ceux qui ont installé des extensions comme Download Statusbar et Greasemonkey, en mode « Flat », c'est-à-dire que les fichiers générés ne sont pas stockés dans une archive .jar (ndlr : presque toutes les extensions fonctionnent sur ce principe). Ils peuvent alors être visités et consultés par un internaute malveillant.

Les chercheurs de bugs de Mozilla estiment que le risque associé à cette menace est **faible** et ils travaillent sur un correctif. Pour se protéger, les utilisateurs de Firefox peuvent utiliser l'extension GPL NoScript qui bloque les codes malveillants. Car, tant qu'un site Web plombé par du code malveillant n'a pas été ajouté à la liste des sites fiables reconnus par l'utilisateur cela devrait permettre d'empêcher les attaques de fonctionner.

Le fait de visiter une page Web frauduleuse est un risque puisqu'elle est capable de charger des images, des scripts et tous types de données non compressées qui sont stockées dans un endroit précis du disque dur, un répertoire dont l'utilisation est récurrente.

Certaines extensions Firefox stockent des données dans des fichiers Javascript et un attaquant peut également les retrouver. Selon Eisenhaur, les scripts des utilisateurs de Greasemonkey peuvent être consultés avec cette méthode. Par contre, le stockage des sessions Web et les préférences de l'utilisateur ne peuvent être consultés via cette technique. Reste que selon lui, cette vulnérabilité peut à terme devenir très dangereuse.