Google corrige une faille critique dans son navigateur Chrome

Si Google fait évoluer rapidement les versions de développement de son navigateur Chrome, l'actualité concernant la mouture stable est plutôt réduite.

La compagnie dévoile toutefois aujourd'hui la mouture 1.0.154.59 de Google Chrome. Celle-ci corrige **un bogue critique**. Une page infectée, lue dans Internet Explorer, peut provoquer le démarrage de Google Chrome et l'affichage de n'importe quelle adresse ou le lancement de code JavaScript.

Dans la pratique, cela permet d'exécuter un code JavaScript sur un autre site que celui où il a été chargé initialement (***cross-site scripting***). Il est aussi possible de lister le contenu du disque dur de l'utilisateur (**dossiers et fichiers**) et de transmettre ces informations à un site web externe.

Cette faille a été découverte par **Roi Saltzman**, de l'IBM Rational Application Security Group, lequel propose un rapport d'une rare précision (problématique, méthodes d'exploitation et exemples de mise en œuvre). En le parcourant, nous remarquons que Google aura mis presque un mois pour corriger cette vulnérabilité, ce qui reste dans la moyenne constatée chez d'autres éditeurs.

Google Chrome est aujourd'hui **en phase de croissance**. L'indice proposé par Market Share fait ainsi apparaitre des parts de marché de 1,23 %, en hausse rapide, quoique loin derrière les chiffres d'Internet Explorer, Firefox ou Safari. StatCounter, place pour sa part Chrome en cinquième position avec 1,96 % de parts de marché. Attention toutefois, car – là encore – ces parts de marché sont en croissance très rapide.