Alerte : une vulnérabilité affecte Google, MSN Live et Yahoo search

La vulnérabilité a été découverte alors que les ingénieurs du CSRT analysaient le contenu du site Web piraté d'une université, contenu qui a été nettoyé par la suite.

Le code malicieux était toujours présent et actif depuis les pages en 'cache' hébergées par les moteurs de recherche.

Selon le communiqué de l'éditeur :*« La plupart des moteurs de recherche ne vérifient pas la sécurité du code contenu dans les pages Web conservées en 'cache', et la menace est là. Les pages Web en 'cache' sont sauvegardées en intégrant les scripts et le code HTML qui peut également contenir différentes vulnérabilités. »*

Si la page Web actuelle a changé, il y a des chances pour que la page en 'cache', elle, soit une ancienne version. Si les pages Web ont été supprimées ou bloquées par un filtre d'adresses URL ou une liste noire d'un FAI, les pages en cache, elles, sont toujours accessibles lorsque l'on clique sur les liens de l'option « en cache » dans les résultats proposés par les moteurs de recherche, puisque les liens vers ces pages sont différents de ceux qui dirigent vers la page Web actuelle.

Les pirates sont également capables de concevoir des assauts durant lesquels ils vont délibérément attaquer les liens, créer des *pop-ups* ou des *frames* Windows «invisibles» qui contiennent du code directement issu des pages Web en 'cache' que propose le moteur de recherche.

Enfin, cette vulnérabilité peut aussi contourner les solutions de filtrage d'URL qui ne bloquent pas les pages Google par exemple.