Google Search Appliance cache une faille

Un bug dans l'outil de recherche de Google mettrait en péril plusieurs sites internet.

Des experts ont lancé une alerte. La découverte d'une vulnérabilité dans Google Search Appliance, une solution prisée par de nombreuses organisations comme les banques ou les universités qui permet d'ajouter un moteur de recherche sur un site web, est une très mauvaise nouvelle pour les administrateurs de pages internet.

La faille, qui concerne la façon dont le système gère certains caractères, permettrait à un attaquant d'insérer un lien web qui fait croire à l'internaute qu'il est redirigé vers un site sécurisé. Seulement dans la réalité, le site contient du code malveillant.

D'après John Herron, un expert en sécurité qui s'occupe du site NIST.org, : *» Cette vulnérabilité touche un grand nombre de sites. Elle permet à un attaquant de défacer le site, de le rendre illisible. »*

Elle ouvre également la porte aux cybercriminels spécialisés dans le phishing ou hameçonnage. Traditionnellement les scams de phsihing utilisent des mails contenant des liens renvoyant vers de faux sites. L'utilisation détournée du bug dans Google Search Appliance reprend ce système, mais sans avoir à utiliser de courriel.

Ce problème de cross-site scripting (XSS) concerne le caractère d'encodage 7-bit, l'UTF pour Unicode Tansformation Format, *« ce qui rend cette vulnérabilité particulièrement sensible »* estime, Jeremiah Grossman, chef de la technologie pour WhiteHat Security.

« Google a découvert le problème la semaine dernière » précise un porte-parole du groupe dans un courrier électronique. *« Nous avons envoyé une note à tous nos consommateurs dés le 22 novembre, avec des explications précises pour se protéger. »*

Pour l'instant Google déclare ne pas être au courant d'une attaque exploitant de bug. Le groupe semble avoir réagi promptement, mais il doit poursuivre son effort d'information.

Pour se protéger, les internautes doivent absolument inspecter et surveiller les liens web de leurs sites. Normalement, les faux liens sont particulièrement long, et donc plus facilement identifiables. En cas de doute, autant abandonner et envoyer un mail au webmaster du site pour lui signaler le problème.