Google publie un correctif pour Gmail

Un hacker peut tout à fait créer un site Web malveillant dont la mission sera de copier la totalité des noms et adresses présents dans l'annuaire d'un utilisateur Gmail qui s'y connecte .

Ces données sont un véritable trésor pour les spammeurs puisqu'ils peuvent par la suite mieux cibler leurs futures victimes. La condition *sine qua non* pour récupérer les précieuses données étant que l'utilisateur cible soit connecté sur le site au moment de la récupération des identifiants.

Ce problème a été découvert à la suite de l'ajout d'une fonction dans Google Video. Cette dernière nommée *'Pick to People Email'*permet aux utilisateurs de piocher dans leurs contacts Gmail pour se faire suivre un lien vidéo.

Seulement cette fonction déjà très utilisée sur les sites communautaires comme *YouTube*ou *MySpace*ouvre également l'annuaire aux autres internautes ce qui en terme de sécurité est dramatique.

Heather Adkins, le manager de l'information sécurité de Google a confirmé la présence de cette faille et qu'un correctif a été publié dans un délai très court.

Dans un mail, Adkins indique :*« À notre connaissance personne n'a exploité cette vulnérabilité et aucun des utilisateurs de Gmail n'a été touché. «*

Ce bug existe à cause de la façon dont Gmail gère le JSON (*JavaScript Object Notation* – Notation des objets issus de JavaScript) un format léger d'échange de données.

D'après Adkins, *« ces objets, s'ils ne sont pas correctement utilisés peuvent mettre en péril certaines données confidentielles. Avec le correctif que nous avons déployé, cela est désormais impossible. »*

Google doit régulièrement corriger les failles découvertes dans ses services. Dans la plupart des cas, elles sont relativement récentes et exploitent les faiblesses des nombreuses applications Web.

Par exemple les bugs CSS (*Cross Site Scripting*) qui ciblent l'internaute et non les serveurs qu'ils utilisent. Les attaques CSS peuvent faciliter le travail d'un spécialiste du phishing.