Cloudflare : une coquille dans le code expose des données utilisateurs

Une erreur de frappe dans le code source d'un composant de CloudFlare a exposé des données personnelles d'utilisateurs de sites web utilisant les services de CloudFlare (CDN, sécurité…). Les informations exposées comprennent aussi des éléments plus sensibles comme les cookies, les mots de passe, des token d'authentification, des requêtes HTTP, des clés de chiffrement, etc. Cette fuite de données a été découverte par Tavis Ormandy, du project zero de Google. Selon lui, la liste des services web concernés par ce que les spécialistes appellent déjà le « cloudbleed » est longue. Elle comprend notamment, Uber, 1Password, FitBit, OKCupid, etc.

Une faute de frappe

Après analyse, nos confrères de *Bleepingcomputer* rapportent que l'erreur de typographie était dans le composant HTML Parser de CloudFlare. Ce module est utilisé pour lire le code source d'un site web pour modifier une page. Comme par exemple basculer automatiquement de HTTP en HTTPS. Un développeur a écrit dans le code « = = » au lieu de « >= ».

Une simple faute mais avec comme conséquence que le parser HTML a provoqué un débordement de tampon. Une partie des données présentes dans la mémoire vive du serveur CloudFlare a été intégrée dans les requêtes HTTP, donc accessible et référencée sur Internet. Dans son enquête, Cloudflare souligne que ce problème est apparu quand les clients ont activé deux paramètres dans leur compte : Email Obfuscation et Automatic HTTPS Rewrites

5 mois de durée, mais 0,00003% des requêtes concernées

Le bug a duré 5 mois. La faute de frappe a été introduite dans HTML Parser le 22 septembre 2016 et le chercheur de Google a alerté CloudFlare qui a immédiatement réparé le 18 février 2017. John Graham-Cumming, CTO de CloudFlare, dans un blog, a relativisé l'incident. « *L'activité la plus intense du problème de fuite de mémoire a été entre le 13 et 18 février en impactant 1 requête chaque 3,3 millions de requêtes HTTP, cela représente donc 0,00003% des demandes.* » Le dirigeant souligne que le bug a été résolu en 47 minutes après sa découverte en désactivant dans un premier temps, les deux paramètres touchés. Il a fallu ensuite 6 heures pour identifier la typographie défaillante.

Dans son rapport Tavis Ormandy donne des captures d'écran de données glanées sur les moteurs de recherche. « *J'ai découvert des messages privés de grands sites de rencontres, des discussions d'un service de chat connu, des informations de gestionnaires de mots de passe en ligne, des réservations d'hôtels, etc.* » Le chercheur ne sait pas si « *ce problème a été remarqué et exploité, mais je suis sûr que d'autres crawlers (robot d'indexation) ont collecté des données et que les utilisateurs ont sauvegardé ou mis en cache des contenus sans réaliser ce qu'ils ont* ». Pas de quoi rassurer !

A lire aussi :

2017 : la seconde de plus qui a déboussolé Cloudflare

Pour CloudFlare, 94% du trafic du réseau Tor est malveillant

crédit photo © andriano.cz – shutterstock