Google ignore la colère de Microsoft en publiant une autre faille Windows

En début de semaine, Microsoft piqué une colère contre Google qui avait dévoilé une faille de type zero day dans Windows 8.1 avant la publication des correctifs du Patch Tuesday. Le problème provient d'une méthode différente entre les deux firmes sur la publication des failles. Google a adopté le modèle de divulgation systématique des détails des vulnérabilités, après un délai jugé raisonnable (Full disclosure). Ce délai est aujourd'hui de 90 jours. Microsoft milite pour un autre modèle, la divulgation coordonnée de failles (CVD pour Coordinated vulnerability disclosure).

Il semble que le coup de sang de la firme de Redmond n'ait eu aucun écho. En effet, la même équipe de Project Zero vient de publier une autre faille dans l**a fonction de chiffrement mémoire, CryptProtectMemory, dans Windows 7 et 8.1**. James Forshaw, le même chercheur qui a découvert la première faille, a décrit ce bug comme le contournement du contrôle de l'usurpation d'identité. « *Lorsque vous utilisez l'ouverture d'une connexion avec (CRYPTPROTECTMEMORY_SAME_LOGON flag), la clé de chiffrement est générée en fonction de l'identifiant pour accéder à cette connexion et pour partager de la mémoire entre les différents processus* ». Il ajoute que « *le problème vient de l'implémentation dans CNG.sys qui ne fait pas la vérification de l'usurpation d'identité au niveau du Token. Il est alors possible pour un utilisateur de contourner ce contrôle et de déchiffrer les données de la session* ».

Cette vulnérabilité a été **découverte le 17 octobre** dernier et Google a averti Microsoft. Ce dernier a été capable de reproduire l'exploit à partir du 29 octobre. Depuis, la firme de Redmond n'a pas publié de correctif pour cette faille et Google fidèle à sa politique a publié les détails du bug. James Forshaw constate : « *Microsoft nous a informé qu'un correctif était prévu dans le Patch Tuesday de janvier, mais ne l'a finalement pas intégré pour des problèmes de compatibilité. Par conséquent, le correctif est maintenant prévu dans le Patch Tuesday de février.* » De quoi rasséréner les relations entre les deux acteurs.

A lire aussi :

Un Patch Tuesday légèrement critique et sans correctifs pour IE
Microsoft : les Patch Tuesday deviennent des guides de piratage de Windows XP

Crédit Photo : Kentoh-Shutterstock