

Pwn2Own : Chrome est tombé... Google verse 60 000 dollars

Chrome n'a pas été à la fête au concours de *hacking* Pwn2Own. Le butineur est ainsi tombé une première fois, suite aux attaques du Français **Vupen Security**.

Une combinaison de failles a été exploitée. Une première pour passer à travers le bac à sable intégré à Google Chrome, et une seconde réduisant au silence les technologies de sécurité intégrées à Windows. Il semblerait qu'un composant Flash ait été utilisé : les points de contact entre l'OS et le navigateur sont ici plus nombreux, réduisant ainsi l'épaisseur de la couche d'isolation du bac à sable (et augmentant d'autant la surface d'attaque).

L'autre faille critique découverte dans Chrome est l'œuvre de **Sergey Glazunov**. Un habitué, puisqu'il décroche régulièrement des récompenses pour la découverte de vulnérabilités dans ce butineur. L'exploit est de taille, car la faille exploitée est « native » (et ne passe donc pas par un greffon). Google a livré un correctif éliminant les deux bogues liés à cette faille, et versé 60 000 dollars à Sergey Glazunov.

Pour les dollars, il faudra jouer le jeu

La version 17.0.963.78 de Chrome, accessible pour Windows, Mac OS X et Linux, corrige ce problème et devra donc être installée sans tarder.

En offrant 60.000 dollars à Sergey Glazunov et rien (pour le moment) à l'équipe de Vupen Security, Google [marque son désaccord](#) envers les règles du concours Pwn2Own, qui permettent aux *hackers* de dévoiler une faille sans expliquer quels bogues ont été exploités.

Une pratique contestable, car elle empêche les éditeurs de trouver rapidement une parade aux problèmes constatés, laissant d'autant plus longtemps les utilisateurs à découvert.