



Éditorial

Month of Bugs

Guillaume Lehembre 

Depuis presque un an, plusieurs chercheurs en sécurité ont lancé la divulgation de failles à thème chaque jour d'un mois donné. Ces initiatives ont pour but de montrer la facilité de trouver des failles de sécurité dans des applications très répandues (navigateurs Internet, langages de programmation, kernels, etc.). Cette « mode » a été initiée par H.D Moore, le développeur principal du *framework* Metasploit, avec son *Month of Browser Bugs* en juillet 2006 suivi d'un *Month of Kernel Bugs* en novembre 2006. Une partie non négligeable de ces failles a été découverte grâce à l'utilisation de méthodes de *fuzzing*. Le *fuzzing* consiste à injecter des données aléatoires à l'entrée d'un programme pour lui faire générer des erreurs pouvant aller jusqu'au plantage du programme. L'analyse des erreurs et de l'entrée correspondante permet alors de découvrir certaines vulnérabilités.

Le coût des tests est négligeable et permet de déceler des failles qu'un testeur humain n'aurait pas trouvés lors d'une campagne de tests approfondie. La dernière initiative d'H.D Moore a permis de développer les *fuzzer fsfuzzer* (systèmes de fichiers) et *sysfuzz* (appels systèmes) en plus des outils déjà existants (Hamachi, CSS-Die, DOM-Hanoi). Les navigateurs Internet représentent très certainement l'une des meilleures portes d'entrée actuelles pour compromettre un système à distance, le choix d'H.D Moore pour ce premier *Month of Bugs* n'a donc certainement pas été anodin :-)

L'initiative du *Week of Oracle Bugs* proposée par Cesar Cerrudo a été ajournée pour des raisons inconnues. Les mauvaises langues diront qu'Oracle a fait pression sur eux ... et pourtant Oracle bat tous les trois mois des records en terme de nombre de failles corrigées (51 vulnérabilités corrigées lors de la mise à jour de janvier 2007 par exemple). Apple a aussi été mis sous les projecteurs en janvier 2007 avec le *Month of Apple Bugs* qui a déjà permis de corriger de nombreuses failles. La dernière initiative en date concerne le très populaire langage de programmation Web PHP. Stéphane Esser, fondateur du groupe PHP Hardened et initiateur du projet, a quitté l'équipe sécurité interne PHP depuis décembre 2006. Il a décidé de lancer le *Month of PHP Bugs* suite aux critiques qu'il avait émises sur le temps de réponse de

l'équipe sécurité vis à vis des bugs sécurité PHP. Voici une liste des principaux *Month of Bugs* en date de mars 2007 :

- *Month of Browser Bugs* – <http://browserfun.blogspot.com> (Juillet 2006),
- *Month of Kernel Bugs* – <http://projects.info-pull.com/mokb/> (Novembre 2006),
- *Week of Oracle Database Bugs* – <http://www.argeniss.com/woodb.html> (Décembre 2006),
- *Month of Apple Bugs* – <http://projects.info-pull.com/moab/> (Janvier 2007),
- *Month of PHP Bugs* – <http://www.php-security.org> (Mars 2007).

Ce type d'initiative ne vas pas s'arrêter en si bon chemin et d'autres thèmes vont être exploités dans un futur proche. Un des aspects moteurs de ces initiatives est le *fuzzing*, qui n'est plus cantonné à éprouver la robustesse des systèmes, mais sert dorénavant à découvrir rapidement des failles de sécurité. Des travaux sont par exemple en cours sur les lecteurs vidéo [1], les protocoles réseaux, etc. On peut aussi souligner l'initiative de Nicolas Ruff pour répertorier sur son *blog* [2] les déboires sécurité du dernier-né des systèmes d'exploitation de Microsoft, avec un titre tout trouvé : *Month of Vista Bugs ! To be continued ...*

Références :

- Zzuf [1] – <http://sam.zoy.org/zzuf/>,
- Month of Vista Bugs [2] – <http://movb.blogspot.com> (Mars 2007).

À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants – <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et a acquis une expérience certaine dans la sécurité des réseaux sans fils. Il a réalisé des interventions publiques sur ce sujet et a publié plusieurs articles, dont un article dans le numéro 14 de hakin9 intitulé Sécurité Wi-Fi – WEP, WPA et WPA2. Il rédige un éditorial mensuel dans Hakin9 depuis Janvier 2007. Guillaume peut être contacté à l'adresse suivante : Guillaume.Lehembre@hsc.fr.