




Patch 0day !

Guillaume Lehembre 

Tout bon administrateur ou responsable sécurité qui se respecte connaît le fameux "Patch Tuesday" qui est devenu depuis quelques temps le rendez-vous mensuel de Microsoft pour ses correctifs de sécurité chaque deuxième mardi du mois.

On savait bien que les chercheurs sécurité attendaient impatiemment la sortie des différents correctifs Microsoft pour faire une analyse différentielle des fichiers modifiés afin de créer une preuve de concept d'un code d'exploitation, mais depuis quelques temps la "mode" est passée à la divulgation de code d'exploitation aux environs du "Patch Tuesday". Ces divulgations ciblées ont pour but d'exploiter la vulnérabilité pendant le plus de temps possible et de forcer Microsoft à sortir un correctif de sécurité hors cycle (ce qui reste très rare). Les exemples les plus célèbres sont certainement les vulnérabilités ayant touchées Internet Explorer ces derniers mois : la faille WMF (MS06-001) fin 2005 / début 2006 ou encore la faille WML (MS06-055) en septembre 2006. Ces failles ont fait grand bruit dans la communauté sécurité, à un point tel que des correctifs alternatifs ont été recommandés par plusieurs institutions du domaine (CERT, etc.). C'est évidemment la criticité des failles et leur exploitation massive au quatre coins du Web qui ont poussé certaines pointures du monde de la sécurité, comme Ilfak Guilfanov, à sortir un correctif non officiel pour la faille WMF et à se regrouper par la suite au sein du *Zeroday Emergency Response Team* (ZERT) [1]. L'intérêt de tels groupes est aussi de proposer des correctifs critiques pour des systèmes d'exploitation qui ne sont plus supportés comme cela a été le cas avec la faille WML. Des systèmes comme Windows NT4 sont encore relativement répandus en entreprise et plus aucun correctif de sécurité officiel n'est proposé. Et pourtant, des failles comme celle touchant le service Server (MS06-040) ont des codes d'exploitation publics et fiables pour exploiter ces systèmes. La solution vient alors d'une souscription au programme *Microsoft Custom Support Agreement* (CSA) réservé aux grand comptes en cours de migration ... mais pour les autres une migration rapide vers des systèmes supportés s'impose.

Dorénavant plus un mois ne passe sans qu'une faille 0day ne soit exploitée dans un produit Microsoft

et cela n'est pas près de changer. Les vecteurs privilégiés sont le navigateur Web Internet Explorer ou les différents programmes de la suite Office (Word, Excel, Powerpoint). L'appât du gain rapide via l'installation de programme de type spyware est l'une des principales motivations des personnes divulguant ses failles de manière non responsable.

Depuis maintenant quelques temps, des sociétés comme *iDefense* (rachetée par *Verisign*) ou *Tipping-Point* (3com) via leur programme nommé "Zero Day Initiative" rémunèrent les chercheurs en sécurité pour avoir la primeur de leur découverte en matière de faille de sécurité. Les vulnérabilités sont alors échangées au sein d'un club restreint de souscripteurs et divulguées par la suite publiquement.

Les bons 0days se monayent donc très chers et ceux qui les découvrent sont de plus en plus tentés de les utiliser à mauvais escient pour en tirer le plus de bénéfices possible. Il apparaît donc nécessaire de suivre l'actualité sécurité au plus près pour connaître les nouvelles menaces et les éventuelles parades avant l'arrivée d'un correctif.

Donc sortez couvert et n'oubliez pas d'appliquer les correctifs de sécurité (même si cela ne suffit pas toujours) :-)

- <http://zert.isoft.org/> [1]

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". Guillaume peut être contacté à l'adresse suivante : Guillaume.Lehembre@hsc.fr.