http://daffyduke.lautre.net/spip/?1er-challenge-pirate-moi-com-5h

1er challenge pirate-moi.com : 5h ont suffi

- 6- Webographie -

Date de mise en ligne : vendredi 21 janvier 2011

Le premier concours d'intrusion mis en ligne par pirate-moi.com a été un succès. C'est le CMS SPIP qui a été mis en pature et c'est au bout de 5h seulement qu'une faille a été découverte et remportée par un jeune homme de 19 d'à peine 18 ans identifié sous le pseudo de "Matsuyama".

En continuité d'un article précédent sur pirate-moi, quelques précisions suite à un échange téléphonique avec Eric Seguinard il y a quelques jours.

L'objectif de pirate-moi.com est de tester la sécurité d'applications de gestion de contenu de sites Internet. L'approche est pragmatique : Une application est sélectionnée et sa dernière version est déployée sur les serveurs de pirate-moi.com. Dès le lancement du concours les personnes inscrites découvrent l'application et se mettent à chercher des failles de sécurité.

Le premier ayant réussi à trouver une faille remporte le concours : A la clef, la reconnaissance de ses compétences auprès de ses pairs et une interview par Eric Seguinard ; la personne de securi-toile à la source de cette idée. Si l'application testée a été sponsorisée par une entreprise le gagnant bénéficie aussi d'un prix (dans le cadre du concours de Janvier c'était un iPad qui été mis en jeu).

Analyse du challenge

Pour le premier challenge, le choix s'est porté sur le CMS SPIP dans sa version 2.1.5 (version publiée le 22 décembre 2010). Ce gestionnaire de site web est très utilisé dans la communauté Internet Française.

Pour trouver la faille, le gagnant du concours s'est appuyé sur une analyse du code source de l'application, celui-ci étant en opensource. Une fois son angle d'attaque identifié, celui-ci a lancé son attaque sur l'application en ligne et a remporté le concours après vérification de la part des organisateurs.

La faille découverte permettait à une personne ayant le profil de rédacteur de modifier la configuration et l'apparence du site (langue, nom du site, description, ...) ; actions normalement réservées à un profil de gestionnaire du site. Autrement dit, il s'agit d'une "escalade de privilège" (privilege escalation).

Retombées du concours

Au total, deux failles ou trous de sécurité ont été ainsi découvertes (celle de Matsuyama et une autre par Eric Seguinard de securi-toile). C'est Eric qui s'est chargé de valider les failles pour ensuite les remonter aux personnes derrrière le logiciel SPIP. La réaction ne s'est pas fait attendre : 24h après, la version 2.1.6 de SPIP était annoncée et corrigeait les problèmes remontés. Chapeau !

Challenge de Février : Plateforme de e-commerce

Le challenge de février portera sur une application permettant de monter des boutiques Internet : Gestion du catalogue, application de caddie, gestion des livraisons et de la facturation, des paiements. Le nom de l'application est gardé secret afin que personne ne prenne l'avantage avant le début du concours. Clairement une bonne précaution au vu du délai de 5h qui a été suffisant pour le premier challenge.

Lors du 1er challenge, c'est près de 400 participants qui se sont inscrits, 50 se sont connectés et seulement 12

d'entre-eux ont créé un compte rédacteur qui permettait de s'ouvrir la voie à des attaques plus évoluées. La faible participation pouvant être expliquée du fait que le challenge démarrait le 1er Janvier à 0h00 : Seuls les plus motivés était devant leur clavier en plein réveillon !

Afin de facilter et encourager la participation à ce 2nd concours le "top départ" est fixé au samedi 5 février à 9h00 du matin : Cela devrait devrait grandement booster le nombre de "joueurs".

Le difficile parcours des CVE

Si il y aurait un point à améliorer serait celui au niveau des entrées CVE (Common Vulnerabilities and Exposures). En effet, pour les failles remontées aucune entrées dans la base CVE n'ont été créées : Les failles sont donc "inconnues au bataillon" pour de nombreux organismes qui s'appuient sur ce référentiel pour réaliser leur veille sécurité et maintenir à jour leurs systèmes. Un suivi des blogs et annonces de chacun des logiciels utilisés est donc un pré-requis, ou alors il faut se tourner vers des services payants de veille sécurité qui font ce travail contre espèces sonnantes et trébuchantes.

Faire créér des entrées CVE n'est pas aussi simple que cela : Il faut passer via des entitées reconnues (un CERT ou un grand éditeur de logiciels) pour obtenir une entrée CVE. A par les gros projets OpenSource c'est un peu le chemin de croix... pour in-fine, pas ou peu de retour mis à part voir son projet/logiciel identifié comme un mauvais élève car "ayant eu des vulnérabilités".... Les mauvaises langues pourraient dire que c'est fait exprès pour passer sous le radar...

Dans le cas de la faille découverte par Matsuyama dans SPIP 2.1.5, qui a été corrigée dans la 2.1.6, aucune entrée CVE n'a été créée. Ce qu'il est intéressant de noter c'est que la correction a été néanmoins taggée dans l'avis Secunia SA42909 émis le 17 Janvier 2011.

En conclusion, les services commerciaux de veille sécurité ont de beaux jours devant eux !

Sécurité applicative : un challenge actuel amené à empirer

Clairement, les failles de niveau applicatives sont LE challenge de demain (avec la sécurité des périphériques mobiles, les systèmes industriels et objets connectés, ...). Si rien n'est fait pour faciliter ce travail de référencement et de communication pour faciliter la mise à jour des applications et systèmes en place, le problème ne va aller qu'en s'aggravant.

Déjà qu'il n'est pas simple de faire patcher les systèmes dans des délais corrects, ce sera pire si l'information de base concernant une nouvelle vulnérabilité reste coincée quelque part dans un blog ou une liste de distribution...

Pour aller plus loin

Pour en savoir plus sur les procesus de gestion des vulnérabilités je vous encourage à consulter la série d'articles d'Alexandre Lauga sur le sujet :

Security Patch Management [1/3] : effet de mode ou besoin réel ?

Security Patch Management [2/3] : problématique et écueils à éviter

Security Patch Management [3/3] : le processus idéal

Cet article est repris du site http://blogs.orange-business.com/se...