Qualys annonce BlindElephant, un outil Open Source pour identifier les applications Web

Ce nouveau moteur accélère et affine l'identification des applications Web

Black Hat, Las Vegas, NV – le 28 juillet 2010 – Qualys, Inc. le principal fournisseur de solutions à la demande pour la gestion des risques de sécurité informatique et de la conformité, annonce BlindElephant, un moteur Open Source rapide et précis pour identifier les versions des applications Web et des plug-ins à l'aide de fichiers statiques. En marge de cette annonce, des travaux d'analyse seront dévoilés à l'occasion de Black Hat USA 2010 sur les résultats de tests à grande échelle de cet outil qui démontrent l'utilisation de logiciels non mis à jour mettant en danger de nombreuses applications Web bien connues.

De nombreuses applications Web classiques sont utilisées dans différents domaines, notamment pour gérer des blogs ou des forums, faire de l'e-commerce, gérer des bases de données ou envoyer ou recevoir du courriel. De par leur nature, ces applications présentent des risques de sécurité spécifiques. Et dans la mesure où toujours plus de vulnérabilités sont découvertes, il est important de pouvoir détecter de manière fiable les applications et les plug-ins utilisés sur un site ainsi que l'utilisation de versions non actualisées. Contrairement à d'autres outils destinés aux applications Web, BlindElephant utilise une nouvelle stratégie qui s'appuie sur le « hashage » de fichiers de ressources statiques au sein de l'application pour trouver un numéro de version.

« Les applications Web standards sont régulièrement ciblées par les pirates puis corrompues pour distribuer des codes malveillants, » déclare Wolfgang Kandek, CTO de Qualys. *« Nous diffusons l'outil BlindElephant en tant que projet Open Source qui permettra aux entreprises de se protéger et de superviser leurs applications Web. Il s'agit d'une première collaboration avec la communauté dans le but d'augmenter le nombre d'applications Web identifiées. »*

« *Avec BlindElephant, les professionnels de la sécurité et les administrateurs système identifient tout ce qui tourne sur leurs serveurs, notamment toutes les applications Web que les utilisateurs ont pu télécharger, »* déclare Patrick Thomas, expert sécurité chez Qualys et créateur de BlindElephant. *« Cet outil ne vérifie pas les vulnérabilités ni l'exposition des applications à un exploit spécifique mais les versions de celles-ci exécutées sur un site. »*

Quelques avantages de BlindElephant :

- Intervention manuelle réduite pour la prise en compte et l'identification de nouvelles versions/applications
- Résistance au durcissement (suppression de bannières)
- Détection fine pour réduire les faux positifs et les faux négatifs
- Réutilisation du même code pour toutes les applications prises en charge
- Vitesse et gestion de la charge pour une utilisation sur le plus grand nombre d'applications
- Faible utilisation des ressources

Pour chaque application supportée par cet outil, BlindElephant conserve un grand nombre de versions de répertoires. Tous les fichiers et les répertoires sont traités puis un « hash » est calculé pour chaque fichier. Ce « hash » est stocké dans une table temporaire avec le chemin et la version de l'application d'origine. La précision de l'outil a été prouvée via une analyse à grande échelle sur des sites visibles sur Internet. Les résultats de l'analyse comprennent des informations sur les applications Web actuellement supportées qui sont les plus utilisées ainsi que la distribution de leurs versions.

L'analyse s'est concentrée sur certaines applications Open Source parmi les plus populaires et

notamment :

- Drupal (système de gestion de contenu)
- Joomla! (système de gestion de contenu)
- Mediawiki (logiciel Wiki)
- Moodle (système de cours virtuels)
- MovableType (logiciel de blog)
- phpBB (logiciel de forum)
- phpMyAdmin (logiciel de gestion de bases de données)
- SPIP (système de gestion de contenu)
- Wordpress (logiciel de blog)

Et Patrick Thomas d'ajouter : *« Le but de cet outil est de fournir un « état des lieux » plutôt que de signaler les vulnérabilités spécifiques d'une application. »*

Disponibilité

Patrick Thomas présentera BlindElephant et ses travaux d'analyse lors d'une session de 70 minutes le 28 juillet à 15h15 (heure d'été du Pacifique) pendant l'événement Black Hat USA 2010.

BlindElephant est un outil Open Source immédiatement disponible en téléchargement sur http://blindelephant.sourceforge.net/.

Pour télécharger les travaux de recherche sur BlindElephant ou obtenir plus de détails, rendez-vous sur le site de la communauté Qualys à l'adresse :
http://community.qualys.com/community/blindelephant

Cette technologie d'identification est actuellement disponible dans QualysGuard Vulnerability Management.

A propos de Qualys

Qualys® Inc est le principal fournisseur de solutions « à la demande » pour la gestion des vulnérabilités et de la conformité sous la forme de services (SaaS). Déployables en quelques heures seulement, partout dans le monde, les solutions SaaS de Qualys fournissent aux entreprises une vue immédiate et permanente de l'état de leur sécurité et de leur conformité.
Actuellement utilisé par plus de 4000 entreprises dans 85 pays, dont 42 des 100 premières sociétés mondiales du classement établi par Fortune, le service QualysGuard® réalise plus de 500 millions d'audits IP par an. Qualys a opéré le plus important déploiement de ressources de gestion des vulnérabilités au monde au sein d'une société figurant parmi les 50 premières entreprises mondiales du classement Fortune.
Qualys a signé des accords stratégiques avec des fournisseurs de services d'infogérance (« managed services ») de premier ordre et des cabinets de conseil tels que BT, Etisalat, Fujitsu, IBM, I(TS)2, LAC, NTT, SecureWorks, Symantec, Tata Communications et TELUS.
Plus d'information sur www.qualys.com