Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 23 novembre 2012
N° CERTA-2012-ACT-047

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-047

1 Compromission de serveurs de FreeBSD

Le week-end dernier, le site freebsd.org a annoncé avoir détecté une intrusion sur son infrastructure. L'attaque aurait eu lieu le 19 septembre 2012, mais n'aurait été détectée que le 11 novembre 2012. Elle serait due à la fuite de la clef SSH d'un développeur.
La base du projet FreeBSD, c'est-à-dire le noyau, les bibliothèques système, le compilateur, les outils en ligne de commande et les démons tels que ssh et sshd, n'aurait pas été touchée. En revanche, le service distribuant les logiciels tiers aurait été ciblé par cette attaque. Il y a donc un risque significatif que ceux-ci aient été modifiés durant la compromission.

Par conséquent, tout système FreeBSD contenant des applications tiers, mises à jour entre le 19 septembre 2012 et le 11 novembre 2012, doit être considéré comme potentiellement compromis. Le CERTA recommande donc de réinstaller complètement le système d'exploitation des machines se trouvant dans ce cas de figure. Suite à cet incident, le système de mise à jour csup/CVSup a été rendu obsolète. Il est donc fortement conseillé de migrer vers *portsnap* ou *subversion*.

Documentation

Annonce officielle de FreeBSD :

http://www.freebsd.org/news/2012-compromise.html

2 Rootkit noyau injecteur d'iframes

La semaine dernière, un administrateur de serveur Web sous Linux, qui enquêtait sur la présence d'*iframes* malveillantes injectées dans les pages a découvert que cette injection était réalisée par un module noyau intégrant des fonctionnalités de *rootkit*.

Ce module est capable en effet d'intercepter les communications réseau au niveau du noyau linux pour modifier les pages HTML renvoyées aux clients. Le code malveillant ajouté peut être reconfiguré par un serveur de contrôle et de commande distant. Les fonctionnalités de *rootkit*

du malware permettent au module de camoufler au système utilisateur certains de ses processus et fichiers de travail. Enfin, la pérennité du malware est assurée par un mécanisme qui force le rechargement du module malveillant à chaque redémarrage du système.

La particularité de cette méthode, originale pour ce type d'attaque, est qu'aucun fichier n'est modifié dans le site Web. Seuls quelques fichiers aux noms « anodins » sont présents dans l'arborescence, et sont masqués aux administrateurs par les fonctions de *rootkit*.

Bien que ce malware ne révolutionne aucune technique de compromission, il montre qu'il est nécessaire de mettre en place des mesures de sécurité particulières aux serveurs de production sous Linux. Par exemple le blocage de chargement de modules noyau à chaud aurait empêché l'attaquant d'ajouter son module malveillant. Il suffit pour cela d'écrire 1 dans `/proc/sys/kernel/modules_disabled`. Cette mesure est décrite dans le document *Recommandations de sécurité relatives à un système GNU/Linux* disponible sur le site de l'ANSSI.

Documentation

– Recommandations de sécurité relatives à un système GNU/Linux :

http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/systeme-d-exploitation-linux/recommandations-de-securite-relatives-a-un-systeme-gnu-linux.html

3 Le cloisonnement se démocratise sous Linux

Cette semaine, le cloisonnement (*sandboxing*) sous Linux s'est renforcé avec la sortie d'une nouvelle version du navigateur Chrome. La particularité de cette version, est l'intégration de nouveaux mécanismes de cloisonnement basés sur une fonctionnalité du noyau Linux appelée « seccomp-bpf » (*Secure Computing Berkeley Packet Filter*).

Pour rappel, le cloisonnement (*sandboxing*) limite les possibilités d'action et restreint les privilèges d'un processus. Le but de cette fonctionnalité est de limiter les dégâts d'une éventuelle exploitation de vulnérabilité dans un processus utilisateur.

La fonctionnalité « seccomp-bpf » est apparue dans le noyau Linux le 11 Janvier 2012. Le langage BPF (*Berkeley Packet Filter*) initialement conçu pour mettre en place des filtres sur les paquets réseau a été adapté au cloisonnement de processus avec « seccomp ». Au lieu de faire des vérifications et des opérations sur les paquets réseau, le langage BPF pour « seccomp » permet de les faire sur les registres processeur. Cela permet de faire des traitements fins au niveau des appels système. Un exemple concret est par exemple de limiter l'appel système « __NR__read » seulement sur le descripteur de fichier « stdin ».

Cette fonctionnalité n'est disponible qu'à partir des noyaux Linux version 3.5, mais a été intégrée dans la version 12.04 LTS de Ubuntu.

De plus en plus de programmes sous Linux commencent à utiliser cette fonctionnalité, on peut citer des logiciels comme vsftpd, OpenSSH. En ce qui concerne Mozilla Firefox, une équipe travaille sur ce sujet, on peut donc s'attendre dans une prochaine version à une évolution vers cette technologie.

Le CERTA recommande l'utilisation de programmes stables utilisant des concepts de cloisonnement et encourage les développeurs à cloisonner leurs applications en espace utilisateur.

Documentation

– Article « A safer playground for your Linux and Chrome OS renderers » du 19 novembre 2012 :
http://blog.chromium.org/2012/11/a-safer-playground-for-your-linux-and.html

– Article « Yet another new approach to seccomp » du 11 janvier 2012 : http://lwn.net/Articles/475043/
– Article « Seccomp and sandboxing » du 13 mai 2009 : http://lwn.net/Articles/332974/
– Article « A library for seccomp filters » du 25 avril 2012 : http://lwn.net/Articles/494252/
– Article « vsftpd-3.0.0 and seccomp filter sandboxing is here ! » du 09 avril 2012 : http://scarybeastsecurity.blogspot.fr/2012/04/vsftpd-300-and-seccomp-filter.html
– Page wiki « Features/Security/Low rights Firefox » : https://wiki.mozilla.org/Features/Security/Low_rights_Firefox

4 Rappel des avis émis

Dans la période du 16 au 22 novembre 2012, le CERTA a émis les publications suivantes :
– CERTA-2012-AVI-656 : Multiples vulnérabilités dans IBM Lotus Notes et Domino
– CERTA-2012-AVI-657 : Multiples vulnérabilités dans IBM Tivoli Management Framework
– CERTA-2012-AVI-658 : Multiples vulnérabilités dans IBM Tivoli Monitoring
– CERTA-2012-AVI-659 : Vulnérabilité dans le système SCADA ABB AC500 PLC
– CERTA-2012-AVI-660 : Multiples vulnérabilités dans les produits Horde
– CERTA-2012-AVI-661 : Vulnérabilité dans Hitachi JP1 Automatic Job Management System
– CERTA-2012-AVI-662 : Vulnérabilité dans Hitachi Device Manager Software
– CERTA-2012-AVI-663 : Multiples vulnérabilités dans VMware ESX et ESXi Server
– CERTA-2012-AVI-664 : Vulnérabilité dans Sophos UTM
– CERTA-2012-AVI-665 : Multiples vulnérabilités dans IBM Business Process Manager
– CERTA-2012-AVI-666 : Multiples vulnérabilités dans IBM IMS Audit Management Expert
– CERTA-2012-AVI-667 : Vulnérabilité dans IBM WebSphere Portal
– CERTA-2012-AVI-668 : Multiples vulnérabilités dans IBM InfoSphere Discovery
– CERTA-2012-AVI-669 : Multiples vulnérabilités dans Opera
– CERTA-2012-AVI-670 : Vulnérabilité dans IBM Intelligent Operations Center
– CERTA-2012-AVI-671 : Multiples vulnérabilités dans IBM Tivoli Access Manager
– CERTA-2012-AVI-672 : Vulnérabilité dans Adobe ColdFusion
– CERTA-2012-AVI-673 : Multiples vulnérabilités dans Oracle Solaris Libxml2
– CERTA-2012-AVI-674 : Vulnérabilité dans Lighttpd
– CERTA-2012-AVI-675 : Multiples vulnérabilités dans IBM Security AppScan Source
– CERTA-2012-AVI-676 : Vulnérabilité dans HP Integrated Lights-Out
– CERTA-2012-AVI-677 : Multiples vulnérabilités dans Autonomy KeyView
– CERTA-2012-AVI-678 : Multiples vulnérabilités dans IBM WebSphere DataPower XC10
– CERTA-2012-AVI-679 : Vulnérabilité dans Oracle Solaris ISC DHCP
– CERTA-2012-AVI-680 : Multiples vulnérabilités dans Mozilla SeaMonkey
– CERTA-2012-AVI-681 : Multiples vulnérabilités dans Mozilla Firefox et Thunderbird édition longue durée
– CERTA-2012-AVI-682 : Multiples vulnérabilités dans Mozilla Firefox et Thunderbird
– CERTA-2012-AVI-683 : Multiples vulnérabilités dans les produits Symantec

Gestion détaillée du document

23 novembre 2012 version initiale.