Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 septembre 2012
N° CERTA-2012-ACT-039

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-039

Gestion du document

Référence	CERTA-2012-ACT-039
Titre	Bulletin d'actualité CERTA-2012-ACT-039
Date de la première version	28 septembre 2012
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Une porte dérobée dans le code source de phpMyAdmin

Le 25 septembre 2012, le bulletin de sécurité *phpMyAdmin* PMASA-2012-5 prévenait les utilisateurs de la présence d'une porte dérobée, ajoutée par un attaquant dans le code source fourni par un serveur mirroir hébergé en Corée. Cette porte dérobée permet à n'importe quel visiteur d'exécuter du code *PHP* sur le serveur sur lequel cette version compromise de *phpMyAdmin* a été installée.

Selon un message des administrateurs de la plateforme d'hébergement, environ 400 utilisateurs ont téléchargé cette version de *phpMyAdmin* à partir du serveur compromis depuis le 22 septembre 2012, date de la compromission.

Le CERTA recommande à toutes les personnes ayant téléchargé *phpMyAdmin* depuis la plateforme *SourceForge* de vérifier l'absence du fichier « server_sync.php » sur leur serveur. Si ce fichier est présent, cela signifie que la version utilisée contient la porte dérobée et qu'un utilisateur malintentionné pourrait prendre le contrôle du serveur. Il est donc impératif de vérifier dans les journaux si ce fichier a pu être accédé, et de réinstaller le serveur à partir d'une sauvegarde saine.

Ce type de compromission, consistant en l'installation d'une porte dérobée dans le code source distribué par des serveurs, se produit régulièrement :

– *ProFTPD* et *phpMyFAQ* en décembre 2010 (voir les bulletins d'actualité CERTA-2010-ACT-048 et CERTA-2010-ACT-050) ;
– des plugins *WordPress*, *VsFTPd* et le noyau *Linux* en 2011 (voir les bulletins d'actualité CERTA-2011-ACT-027 et CERTA-2011-ACT-035) ;

– le projet *Horde* en février 2012 (bulletin d'actualité CERTA-2012-ACT-007).

Il est très difficile de s'assurer de l'inocuité d'un code obtenu sur un site Web sans en effectuer une revue détaillée. Le CERTA recommande, lorsque cela est possible de vérifier les empreintes cryptographiques des logiciels téléchargés. Même si cette vérification n'apporte pas une garantie absolue, car si un serveur est compromis, il est également possible à l'attaquant d'altérer ces empreintes.

Ces évènements nous rappellent que la sécurité d'un produit dépend à la fois de la qualité de son code, et de la qualité de sa chaîne de production et de diffusion.

Documentation

- Billet du blog sourceforge du 25 septembre 2012 :
  http://sourceforge.net/blog/phpmyadmin-back-door/
- Avis CERTA-2012-AVI-523 du 26 septembre 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-523/
- Bulletin d'actualité du CERTA CERTA-2012-ACT-007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-007/
- Bulletin d'actualité du CERTA CERTA-2011-ACT-035 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-035/
- Bulletin d'actualité du CERTA CERTA-2011-ACT-027 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-027/
- Bulletin d'actualité du CERTA CERTA-2010-ACT-050 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-050/
- Bulletin d'actualité du CERTA CERTA-2010-ACT-048 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-048/

2 Correctifs de sécurité et poupées russes

Aujourd'hui de plus en plus de produits intègrent nativement des logiciels ou composants d'autres éditeurs. C'est le cas par exemple du navigateur *Google Chrome* et du navigateur *Microsoft Internet Explorer 10* (logiciels agrégateurs) qui intègrent par défaut le lecteur *Adobe Flash Player* (logiciel intégré). *Adobe Flash Player* n'est pas le seul produit concerné, on retrouve ce phénomène pour *Java, Apache, WebKit* et bien d'autres logiciels ou composants. La conséquence de cette intégration est que les correctifs de sécurité du « logiciel intégré » ne peuvent plus se faire indépendamment de celles du « logiciel agrégateur ».

Pour que le système ne soit plus vulnérable, il faut attendre que les éditeurs se synchronisent. C'est à dire que l'éditeur du « logiciel intégré » livre une mise à jour, et que l'editeur du « logiciel agrégateur » intègre cette mise à jour dans ses propres correctifs. Il est alors possible à l'utilisateur de bénéficier de la correction. Durant ce délai, l'utilisateur est vulnérable.

Il faut savoir que des attaquants étudient la publication des correctifs pour comprendre les vulnérabilités corrigées et ainsi développer des exploits rapidement. Par conséquent, les vulnérabilités corrigées par une mise à jour doivent être considérées comme exploitées et les mises à jour tardives publiées par les éditeurs augmentent considérablement les risques pour leurs utilisateurs.

Dans le pire des cas l'éditeur agrégateur ne met jamais à jour les logiciels intégrés à son produit. Les « logiciels intégrés » dans d'autres produits amènent donc des problématiques de sécurité particulières, car c'est à l'éditeur du « logiciel agrégateur » de prendre en compte leurs mises à jour.

Le CERTA recommande de ne pas acquérir des produits qui ne donnent pas de garantie sur la maintenabilité et en particulier sur le suivi des correctifs de sécurité de leurs composants.

3 Compromission d'un ordiphone par NFC

La technologie de communication sans fil *NFC* (« *Near Field Communication* », « *communication en champ proche* ») peut être utilisée pour effectuer des achats directement avec son téléphone sur un terminal de paiement sans contact, mais également être étendue pour échanger de divers contenus. Ces fonctionnalités augmente donc significativement la surface d'attaque des périphériques mobiles, qui font aujourd'hui face à une exposition déjà très importante.

Plusieurs preuves de concept concernant la prise de contrôle d'un ordiphone en utilisant la technologie NFC ont récemment été démontrées. Une telle attaque nécessite d'être physiquement proche du téléphone de la victime.

Afin de réduire les possibilités d'attaques, le CERTA recommande aux utilisateur de désactiver les services tels que le NFC lorsque ceux-ci ne sont pas utilisés.

4 Codes USSD - Vulnérabilités Samsung et Android

Intégrés sur tous les téléphones portables, les codes USSD (*Unstructured Supplementary Service Data*) permettent d'accéder à certains services de l'opérateur, tels que la consultation du solde du forfait restant. Certaines fonctionnalités utilisant ce système sont directement mises en œuvre par le constructeur du téléphone. La requête est alors traitée par le périphérique lui-même. C'est le cas avec le code `*#06#` permettant d'obtenir l'IMEI du téléphone.

Samsung a mis en place sur certains de ses téléphones un service accessible par un code USSD permettant de réinitialiser et d'effacer les données, sans que l'utilisateur n'ait à confirmer l'action. En effet, le mécanisme de traitement est déclenché dès que le dernier caractère est saisi sur l'interface.

En réutilisant ce code dans un lien spécifique (Web, SMS, QRCode, ...), il est possible de déclencher ce mécanisme à distance en incitant un utilisateur à suivre ce lien. Une mise à jour est en cours de déploiement sur les périphériques Samsung pour imposer une confirmation manuelle lors de l'accès à un service par le biais d'un code USSD.

Le CERTA recommande d'être vigilant lors de la navigation et de ne pas suivre des liens suspects.

5 Rappel des avis émis

Dans la période du 21 au 27 septembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-512 : Multiples Vulnérabilités dans Apple OS X
- CERTA-2012-AVI-513 : Multiples Vulnérabilités dans Safari
- CERTA-2012-AVI-514 : Multiples Vulnérabilités dans IOS
- CERTA-2012-AVI-515 : Vulnérabilités dans Trend Micro InterScan Messaging Security Suite
- CERTA-2012-AVI-517 : Multiples vulnérabilités dans HP SiteScope SOAP
- CERTA-2012-AVI-518 : Multiples vulnérabilités dans les produits Avaya
- CERTA-2012-AVI-519 : Vulnérabilité dans RSA Authentication Agent et Client
- CERTA-2012-AVI-520 : Multiples vulnérabilités dans Joomla!
- CERTA-2012-AVI-521 : Vulnérabilités dans IBM Eclipse Help System
- CERTA-2012-AVI-522 : Vulnérabilité dans IBM WebSphere MQ
- CERTA-2012-AVI-523 : Porte dérobée dans phpMyAdmin
- CERTA-2012-AVI-524 : Multiples vulnérabilités dans AppleTV
- CERTA-2012-AVI-525 : Vulnérabilité dans IBM Informix Dynamic Server
- CERTA-2012-AVI-526 : Vulnérabilité dans IBM WebSphere Application Server
- CERTA-2012-AVI-527 : Vulnérabilité dans Foxit Reader
- CERTA-2012-AVI-528 : Multiples vulnérabilités dans Cisco IOS
- CERTA-2012-AVI-529 : Vulnérabilité dans Cisco Catalyst 4500E Series Switch
- CERTA-2012-AVI-530 : Vulnérabilité dans Cisco Unified
- CERTA-2012-AVI-531 : Vulnérabilités dans Google Chrome
- CERTA-2012-AVI-532 : Vulnérabliités dans IBM WebSphere

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2012-ALE-006-003 : Vulnérabilité dans Internet Explorer (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur)
- CERTA-2012-AVI-516-001 : Vulnérabilité dans Internet Explorer (corrections mineures)

6 Actions suggérées

6.1 Respecter la politique de sécurité

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme. Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel règlementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Quoique puisse suggérer ce document, la politique de sécurité en vigueur dans votre service doit primer.

Cette section précise néanmoins quelques mesures générales de nature à vous prémunir contre les agressions décrites dans ce document. En effet, la sécurité des systèmes d'information ne repose pas exclusivement sur des outils, mais aussi sur une organisation et des politiques.

6.2 Concevoir une architecture robuste

A la lumière des enseignements tirés de ce qui a été présenté dans les bulletins d'actualité, il convient de vérifier que les applications mises en oeuvre (ou à l'étude) ont une architecture qui résiste aux incidents décrits.

6.3 Appliquer les correctifs de sécurité

Le CERTA recommande l'application des correctifs de sécurité.

6.4 Utiliser un pare-feu

L'application des correctifs sur un parc informatique important n'est probablement pas immédiate. Un pare-feu correctement configuré peut retenir certaines attaques informatiques le temps d'appliquer les correctifs. Cependant un pare-feu peut donner une illusion de protection. Cette protection est brisée par la moindre introduction d'un ordinateur nomade dans la partie protégée. On remarque qu'il y a de nombreux paquets rejetés à destination de ports légitimement utilisés par des applications de prise de main à distance. La téléadministration correspond à une demande qui grandit avec la taille du parc à gérer. Les paquets rejetés montrent le risque associé à ce type d'application. Ce risque peut être amoindri par l'usage correct d'un pare-feu.

6.5 Analyser le réseau

De nombreux paquets rejetés étudiés correspondent aux ports ouverts par divers virus/vers/chevaux de Troie. Si votre politique de sécurité autorise le balayage des ports ouverts sur les postes de travail ou les serveurs, il peut s'avérer utile de le faire régulièrement afin de découvrir les machines potentiellement contaminées avant qu'un intrus ne le fasse à votre place.

L'analyse des journaux de votre pare-feu est une source pertinente d'informations pour la sécurité de votre réseau et de vos systèmes. Cela peut vous aider à anticiper des incidents en remarquant par exemple des activités anormales. Le CERTA peut vous aider dans ce travail d'analyse.

6.6 Réagir aux incidents de sécurité

Organisez-vous pour réagir aux incidents de sécurité, en particulier, pour assurer une certaine continuité dans les équipes d'administration et de sécurité.

Le CERTA a pour mission de vous aider à répondre aux incidents de sécurité informatique.

Ne traitez pas les dysfonctionnements des machines à la légère. Dans certains incidents dans lesquels le CERTA intervient, les administrateurs des machines font spontanément part de petits dysfonctionnements inexpliqués et d'apparence anodine qui s'avèrent, au cours de l'analyse, être liés à un incident majeur de sécurité. N'hésitez pas à prendre contact avec le CERTA si vous constatez de l'activité sur les ports décrits ci-dessus.

6.7 Former et sensibiliser les utilisateurs

La sécurité d'un système d'information doit reposer sur une approche de défense en profondeur. Cela signifie, entre autres choses, que l'utilisateur est partie prenante de la sécurité. Sa vigilance, son niveau de formation et de sensibilisation participent à la sécurité du système. C'est pourquoi il est essentiel de prévoir des séances de formation et de sensibilisation des utilisateurs, acteurs de la sécurité. Pour vous aider dans ces actions, l'ANSSI dispose d'un centre de formation :

http://www.ssi.gouv.fr/site_rubrique62.html

Gestion détaillée du document

28 septembre 2012 version initiale.