Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 mars 2012
N° CERTA-2012-ACT-009

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-09

Conditions d'utilisation de ce document :	`http://www.certa.ssi.gouv.fr/certa/apropos.html`
Dernière version de ce document :	`http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-009`

Gestion du document

Référence	CERTA-2012-ACT-009
Titre	Bulletin d'actualité 2012-09
Date de la première version	02 mars 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 Les noms de domaine fantômes

Les cyber-délinquants utilisent souvent des noms de domaine qui pointent vers des serveurs employés, par exemple, à des fins d'hameçonnage ou de distribution de programmes malveillants. Lorsqu'un tel domaine est identifié, une contre-mesure permettant d'arrêter l'activité malveillante consiste à supprimer les références à ce domaine dans les serveurs DNS de plus haut niveau. Cependant des références au domaine restent présentes dans des serveurs DNS de cache jusqu'à ce que les enregistrements arrivent à expiration. C'est pour cette raison qu'une révocation nécessite généralement plusieurs heures avant de devenir globale.

Récemment, une équipe de chercheurs a découvert une vulnérabilité entravant ce mécanisme de révocation en empêchant que les enregistrements arrivent à expiration dans les serveurs DNS de cache. La vulnérabilité affecte la plupart des implémentations de serveurs DNS de cache et est inhérente à la politique de mise à jour du cache. Son exploitation permet à un nom de domaine de rester accessible durant une longue période, même après sa révocation dans les serveurs DNS de plus haut niveau. À cause de la spécificité de ces noms de domaine, révoqués mais toujours accessibles, les auteurs de la découverte ont décidé de les appeler « noms de domaine fantômes » (*ghost domain names*).

L'expérimentation conduite par les chercheurs sur un total de 19045 serveurs DNS de cache ouverts montre que, même une semaine après sa révocation, un nom de domaine peut être maintenu dans 70% des serveurs DNS. Ainsi, en ciblant un maximum de serveurs DNS de cache, les cyber-délinquants pourraient garder leurs noms de domaine malveillants globalement accessibles après révocation. Une autre exploitation de cette vulnérabilité consisterait à cibler un nombre restreint de serveurs DNS de cache, laissant croire que la révocation est effective globalement, mais permettant au nom de domaine de rester accessible à certains endroits.

Pour limiter les risques, le CERTA recommande de ne pas laisser son serveur DNS en accès libre sur l'Internet et d'installer les correctifs lorsqu'ils seront disponibles.

Plus de détails sur la vulnérabilité sont donnés dans la section Documentation.

Documentation

- https://www.isc.org/files/imce/ghostdomain_camera.pdf ;
- implémentations DNS possédant un numéro CVE concernant cette vulnérabilité :
  - *MS 2008* : CVE-2012-1194,
  - *PowerDNS*: CVE-2012-1193,
  - *Unbound* : CVE-2012-1192,
  - *DJBDNS* : CVE-2012-1191.

2 Note d'information sur les défigurations de sites Web

Le CERTA traite régulièrement des défigurations de site Web. L'analyse de ces incidents permet de mettre en évidence la ou les failles exploitées pour modifier le site. La correction des vulnérabilités ainsi découvertes est nécessaire avant toute remise en service du site, afin d'éviter la reproduction de l'attaque.

Le CERTA met à disposition, via son site Web, la note d'information CERTA-2012-INF-002. Celle-ci, intitulée *Les défigurations de sites Web*, propose quelques pistes afin de limiter la surface d'attaque, des techniques de détection des incidents et des mesures de réaction. Une procédure de restauration y est également décrite.

Documentation

- Note d'information du CERTA CERTA-2012-INF-002 du 2 mars 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-002/index.html

3 Rappel des avis émis

Dans la période du 24 février au 01 mars 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-093 : Vulnérabilité dans phpMyAdmin
- CERTA-2012-AVI-094 : Vulnérabilité dans libxml2
- CERTA-2012-AVI-095 : Vulnérabilité dans Bugzilla
- CERTA-2012-AVI-096 : Multiples vulnérabilités dans CISCO SRP 500 Series
- CERTA-2012-AVI-097 : Vulnérabilité dans Python
- CERTA-2012-AVI-098 : Vulnérabilité de CVS
- CERTA-2012-AVI-099 : Vulnérabilité dans Samba
- CERTA-2012-AVI-100 : Vulnérabilité dans IBM AIX
- CERTA-2012-AVI-101 : Multiples vulnérabilités dans PostgreSQL
- CERTA-2012-AVI-102 : Vulnérabilités dans Avaya CMS
- CERTA-2012-AVI-103 : Vulnérabilité dans IBM Personal Communications
- CERTA-2012-AVI-104 : Multiples vulnérabilités dans JP1/Cm2/Network Node Manager i
- CERTA-2012-AVI-105 : Vulnérabilité dans Cisco Cius
- CERTA-2012-AVI-106 : Vulnérabilités dans Cisco Unified Communications Manager
- CERTA-2012-AVI-107 : Multiples vulnérabilités dans Cisco Wireless LAN Controllers
- CERTA-2012-AVI-108 : Multiples vulnérabilités dans Cisco Unity Connection
- CERTA-2012-AVI-109 : Vulnérabilités dans Cisco TelePresence Video Communication Server

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

- CERTA-2012-AVI-087-001 : Vulnérabilité dans libpng (ajout de la référence au bulletin Mandriva)
- CERTA-2012-AVI-094-001 : Vulnérabilité dans libxml2 (rectification du lien Mandriva)

4 Actions suggérées

4.1 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.

4.2 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.

4.3 Appliquer les correctifs de sécurité

Le tableau 2 rappelle les avis du CERTA correspondant aux applications ou codes malveillants relatifs aux ports étudiés dans les sections précédentes.

4.4 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.

4.5 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.

4.6 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.

4.7 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

02 mars 2012 version initiale.