Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 août 2012
N° CERTA-2012-ACT-033

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : CERTA-2012-ACT-033

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-033`

Gestion du document

Référence	CERTA-2012-ACT-033
Titre	CERTA-2012-ACT-033
Date de la première version	17 août 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.

Le bulletin d'actualité est disponible dans son intégralité et au format PDF à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-033.pdf
Un extrait du bulletin, ne reprenant que les articles de la semaine, se trouve en HTML à l'adresse suivante :
http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-033/

1 Mise à jour mensuelle Microsoft

Ce mois-ci deux alertes ont été fermées. La première concerne une vulnérabilité dans *XML Core Services* « CERTA-2012-ALE-003 » et la deuxième touche les serveurs *Exchange* « CERTA-2012-ALE-004 ».
Lors de la mise la mise à jour mensuelle de Microsoft, neuf bulletins ont été publiés. Trois d'entre eux concernant *Internet Explorer*, des composants réseau *Windows* et *Microsoft Common Controls* sont considérés comme critiques.

Les vulnérabilités corrigées permettent :

- l'exécution de code arbitraire à distance ;
- l'exécution de code arbitraire ;
- le déni ce service à distance ;
- l'élévation de privilèges.

Le CERTA recommande l'application de ces mises à jour dès que possible.

Dans un précédent bulletin d'actualité « CERTA-2012-ACT-029 » nous avons évoqué le renforcement de la politique de certificats *Microsoft*. Cette mise à jour optionnelle peut avoir des effets non désirés sur certains réseaux

et empêcher des communications. Nous rappelons donc qu'avant de déployer ce durcissement il faut évaluer son impact sur votre système d'information.

Documentation

- Alerte CERTA-2012-ALE-003 du 14 juin 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-003/
- Alerte CERTA-2012-ALE-004 du 25 juillet 2012 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-004/
- Synthèse des bulletins de sécurité Microsoft du mois d'août 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-aug

2 Des requêtes DNS inattendues

Lorsque l'on navigue sur l'Internet, il arrive que des noms de domaine soient résolus alors qu'aucun site Web associé n'a été visité. Ce phénomène est dû à la conception des navigateurs qui résolvent tous les noms de domaine des liens détectés dans les pages visualisées par l'utilisateur. L'objectif est d'améliorer le temps de réponse si l'un des liens est suivi.

Ce comportement peut poser différents problèmes. Tout d'abord, de nombreuses requêtes DNS seront effectuées inutilement car les liens ne sont pas toujours suivis. Cela entraîne une augmentation significative de la taille des journaux et, par conséquent, peut occasionner des problèmes de stockage et un ralentissement de l'analyse des journaux. Enfin, la visite de sites comportant des liens malveillants provoquera la résolution des noms de domaine associés, ce qui peut donner l'illusion d'un incident alors que le lien n'a pas été suivi.

Cette fonctionnalité, nommée *DNS prefetching*, peut être désactivée :

- par les administrateurs de serveur Web en configurant celui-ci pour envoyer l'en-tête *HTTP X-DNS-Prefetch-Control: off*. Par exemple, sur Apache, le module headers doit être activé et la ligne *Header append X-DNS-Prefetch-Control off* ajoutée dans le fichier de configuration du serveur ou du site Web ;
- par les développeurs de site Web en positionnant la balise *<meta http-equiv="x-dns-prefetch-control" content="off">* dans l'en-tête de la page HTML ;
- par les utilisateurs de Firefox et Chrome (Internet Explorer ne semble pas encore disposer de cette fonctionnalité) :
  - dans Firefox, en tapant about:config dans la barre d'adresses et en créant l'option *network.dns.disablePrefetch* de type booléen et ayant la valeur *true* ;
  - dans Chrome, en tapant *chrome://chrome/settings/* dans l'*omnibar*, en cliquant sur *Afficher les paramètres avancés...* et en décochant *Prédire les actions du réseau pour améliorer les performances de chargement des pages*.

Documentation

- Documentation pour Firefox :
  http://developer.mozilla.org/en-US/docs/Controlling_DNS_prefetching
- Documentation pour Chrome :
  http://www.chromium.org/developers/design-documents/dns-prefetching/#TOC-DNS-Prefetch-Control
- Documentation pour Internet Explorer 9 :
  http://blogs.msdn.com/b/ie/archive/2011/03/17/internet-explorer-9-network-performance-improvements.aspx

3 Rappel des avis émis

Dans la période du 10 août 2012 au 16 août 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-427 : Vulnérabilités dans Google Chrome
- CERTA-2012-AVI-428 : Vulnérabilité dans Xen

– CERTA-2012-AVI-429 : Vulnérabilité dans Oracle Database Server
– CERTA-2012-AVI-430 : Vulnérabilités dans PHP
– CERTA-2012-AVI-431 : Vulnérabilité dans IBM WebSphere MQ
– CERTA-2012-AVI-432 : Vulnérabilité dans Cisco Emergency Responder
– CERTA-2012-AVI-433 : Vulnérabilité dans Cisco IOS
– CERTA-2012-AVI-434 : Vulnérabilité dans libTIFF
– CERTA-2012-AVI-435 : Multiples vulnérabilités dans Internet Explorer
– CERTA-2012-AVI-436 : Vulnérabilité dans Windows Remote Desktop Protocol
– CERTA-2012-AVI-437 : Multiples vulnérabilités dans les composants réseau Microsoft Windows
– CERTA-2012-AVI-438 : Vulnérabilité dans le noyau Windows
– CERTA-2012-AVI-439 : Vulnérabilité dans les moteurs JScript et VBScript de Microsoft
– CERTA-2012-AVI-440 : Vulnérabilité dans Microsoft Office
– CERTA-2012-AVI-441 : Multiples vulnérabilités dans Microsoft Exchange Server
– CERTA-2012-AVI-442 : Vulnérabilité dans Microsoft Visio
– CERTA-2012-AVI-443 : Vulnérabilité dans Microsoft Common Controls

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 CERTA recommande l'application des correctifs de sécurité.

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

17 août 2012 version initiale.