

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-04

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-004>

Gestion du document

Référence	CERTA-2012-ACT-004
Titre	Bulletin d'actualité 2012-04
Date de la première version	27 janvier 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 Note d'information sur les dénis de service

Le CERTA constate une augmentation des attaques en déni de service ciblant ses usagers.

Les attaques informatiques, dont les dénis de service, accompagnent de plus en plus régulièrement les tensions politiques ou idéologiques. L'activité du cyberspace reflète les conflits dont l'actualité est riche.

Empêcher un déni de service est impossible. En diminuer la probabilité et en amoindrir les impacts demandent de la préparation, de l'analyse rationnelle et des réactions appropriées. La note d'information *Dénis de service - Prévention et réaction*, CERTA-2012-INF-001, reprend ces volets et rappelle qu'une indisponibilité peut également résulter d'une cause accidentelle.

1.1 Documentation

- Document du CERTA CERTA-2012-INF-001 du 27 janvier 2012 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-INF-001/index.html>

2 Vulnérabilités dans pcAnywhere

Symantec a récemment publié un correctif pour *pcAnywhere* (voir CERTA-2012-AVI-032). L'une des deux vulnérabilités traitées par cette mise-à-jour est particulièrement critique. En effet, un attaquant peut, par le biais

d'une requête spécifique envoyée au port 5631/tcp de la machine ciblée, provoquer une exécution de code arbitraire à distance. Le CERTA n'exclut pas qu'un ver exploitant cette vulnérabilité apparaisse dans les prochains jours.

Il est recommandé :

- de mettre à jour *pcAnywhere* sur vos postes. Ce logiciel est susceptible d'avoir été installé au travers d'un paquetage (*bundle*), et d'être donc présent sur des machines, à l'insu de leur utilisateur ;
- de filtrer le port 5631/tcp sur les pare-feux, en bordure de réseau comme en interne.

Documentation :

- Avis CERTA-2012-AVI-032 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-032/index.html>

3 Rappel des avis émis

Dans la période du 19 au 26 janvier 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-028 : Vulnérabilité dans OpenSSL
- CERTA-2012-AVI-029 : Vulnérabilité dans Apache Struts
- CERTA-2012-AVI-030 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-031 : Vulnérabilité dans CISCO Digital Media Manager
- CERTA-2012-AVI-032 : Vulnérabilités dans pcAnywhere
- CERTA-2012-AVI-033 : Multiples vulnérabilités dans Opera

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 réglementaire, 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 inexplicables 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

27 janvier 2012 version initiale.