

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-39

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-2010-ACT-039>

Gestion du document

Référence	CERTA-2010-ACT-039
Titre	Bulletin d'actualité 2010-39
Date de la première version	01 octobre 2010
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-2010-ACT-039.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-2010-ACT-039/>

1 Un correctif pour la vulnérabilité dans ASP.NET

La semaine dernière, le CERTA relayait dans son bulletin d'actualité CERTA-2010-ACT-038 la publication d'un bulletin de sécurité de Microsoft concernant une vulnérabilité qui affecte des applications *ASP.NET*. Cette vulnérabilité dans le chiffrement des communications client/serveur permet à une personne malveillante de porter atteinte à la confidentialité de certaines données.

Cette semaine, Microsoft a publié une mise à jour hors cycle afin de corriger cette vulnérabilité. Les informations concernant ce correctif sont disponibles dans l'avis CERTA-2010-AVI-458.

Le CERTA rappelle donc l'impérative nécessité d'appliquer dans les meilleurs délais ce correctif si vous utilisez cette technologie afin de la limiter les risques de fuite d'information.

Documentation

- Avis CERTA-2010-AVI-458 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-458/>

- Bulletin de sécurité Microsoft MS10-070 du 28 septembre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-070.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-070.msp>
- Bulletin d'actualité CERTA-2010-ACT-038 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-038/>

2 Exercice Cyber Storm III : la France s'entraîne avec ses partenaires à faire face à une crise informatique mondiale

Cette semaine, l'ANSSI a participé à l'exercice international organisé par les États-Unis. S'entraîner et se tester sont des actions indispensables à la mise en place d'un plan de gestion de crise SSI cohérent, à sa validation et à son maintien dans le temps. Lors d'un exercice, il convient de limiter les objectifs à tester et de penser à mettre en place des éléments de mesure et des indicateurs permettant d'en qualifier le résultat. Parmi les différents niveaux que l'on peut tester, on retrouve :

2.1 Le niveau technique

Il concerne les applications, les moyens techniques et les personnes. Il peut intégrer, par exemple, un test de pénétration, la vérification que les éléments de surveillance l'enregistrent, que les équipes le détectent et sont capables de le retrouver dans les journaux correspondants (firewall, proxy, ...). Ensuite, il est possible de tester la compréhension de l'exploitation d'une vulnérabilité et la capacité à corriger dans les plus brefs délais.

2.2 Le niveau organisationnel

L'idée est de tester la coordination des équipes et l'efficacité des réactions. Une vulnérabilité fictive peut être annoncée nécessitant une contre-mesure de filtrage qui pourrait avoir un impact métier. La remontée hiérarchique et les communications transverses sont stimulées, l'utilisation de fiches de réaction peut être testée. Une intrusion peut également être simulée pour valider la chaîne juridique (qui sait et peut déposer plainte ?). Il convient aussi de tester les moyens de communication. Les correspondants sont-ils bien identifiés et joignables ? *Les annuaires sont-ils à jour ?* Et si des moyens de communication de secours sont prévus, sont-ils fonctionnels et sait-on les activer ?

2.3 Le niveau décisionnel

Si le niveau technique permet d'identifier qui a la compétence pour débrancher un réseau, il s'agit ici de savoir qui en a la responsabilité décisionnelle. Le choix entre les risques liés à une compromission et l'importance de la disponibilité est dépendant du métier et de la gravité des incidents. Dès lors, il convient de vérifier que les enjeux stratégiques sont connus. Dans ce type d'exercice, le plus compliqué est souvent la remontée d'informations permettant aux décideurs de comprendre la situation le plus justement possible et de réussir à opposer des arguments permettant une réponse réaliste. L'expérience montre que souvent l'importance des réseaux et de l'Internet au bon fonctionnement métier est ignorée et que les impacts d'une coupure de connexion ne sont pas justement perçues.

Bien sûr tous ces exemples sont limités. Tous les cas imaginés et rencontrés au cours des exercices devraient trouver une réponse dans la PSSI locale, sinon c'est l'occasion de la faire évoluer. Le CERTA recommande de réaliser ce type d'exercice en impliquant les équipes locales dans leur organisation. Elles ont la connaissance du métier et des points faibles, techniques et organisationnels.

2.4 Documentation

- Article officiel de la participation de la France à l'exercice Cyber Storm III :
http://www.ssi.gouv.fr/site_article261.html

3 Mise à jour Adobe Flash Player et McAfee

La dernière mise à jour d'*Adobe Flash Player*, rendue extrêmement importante du fait de l'exploitation d'une vulnérabilité du lecteur (voir avis CERTA-2010-AVI-447), confronte les utilisateurs à deux problèmes.

Tout d'abord, l'installation de la dernière version du lecteur *Flash* propose, par défaut, l'installation d'un logiciel tiers, *McAfee Security Scan Plus*. Ce dernier, qui se présente comme un utilitaire gratuit, a la fâcheuse tendance à considérer les éventuels antivirus installés sur le système comme source potentielle de problèmes. Il propose donc d'acheter une suite logicielle plus complète chez l'éditeur *McAfee*. Il est donc fortement conseillé de décocher la case de téléchargement du produit *McAfee Security Scan Plus*.

L'autre problème, plus gênant celui-ci, concerne notamment certains utilisateurs de *Mozilla Firefox* sous *Windows*. Le téléchargement de la dernière version d'*Adobe Flash Player* depuis le site de l'éditeur nécessite de modifier la configuration du navigateur en ajoutant des exceptions (la démarche est expliquée sur le site de l'éditeur). Toutefois, même en suivant à la lettre les explications fournies, le téléchargement ne s'effectue pas toujours correctement. Dans certains cas, un *download manager* est installé mais ne propose aucun téléchargement, dans d'autres cas, absolument rien ne se passe. Au final, les utilisateurs peuvent être tentés de télécharger le lecteur *Flash* sur des sites tiers, sans aucune garantie concernant le logiciel réellement téléchargé. Il est important de savoir qu'*Adobe Flash Player* peut être directement téléchargé sur le site de l'éditeur en suivant l'un des liens ci-dessous :

- pour *Internet Explorer* :
http://fpdownload.adobe.com/get/flashplayer/current/install_flash_player_ax.exe
- pour *Firefox* :
http://fpdownload.adobe.com/get/flashplayer/current/install_flash_player.exe

Documentation :

- Avis CERTA-2010-AVI-447 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-447/>

4 Liens utiles

- Mémento sur les virus :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-002/>
- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>
- Note d'information du CERTA sur les systèmes obsolètes :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-003/>
- Note d'information du CERTA sur les bonnes pratiques concernant l'hébergement mutualisé :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/>
- Note d'information du CERTA sur les mots de passe :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001/>
- Note d'information sur la terminologie d'usage au CERTA :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-002/>
- Note d'information du CERTA sur les enjeux de sécurité liés à une migration vers IPv6 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/>
- Unix security checklist version 2.0 du 8 octobre 2001 (Publication du CERT australien) :
<http://www.auscert.org.au/render.html?it=1937>
- Note d'information du CERTA sur les risques associés aux clés USB :
<http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-006/>
- Note d'information du CERTA sur les outils d'indexation et de recherche :
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-009/>
- Note d'information du CERTA sur la gestion des noms de domaine :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-001/>
- Note d'information du CERTA sur le bon usage de PHP :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-002/>

5 Rappel des avis émis

Dans la période du 24 au 30 septembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-441 : Vulnérabilités dans QuickTime
- CERTA-2010-AVI-456 : Multiples vulnérabilités dans Cisco IOS
- CERTA-2010-AVI-457 : Multiples vulnérabilités dans les produits VMware
- CERTA-2010-AVI-458 : Vulnérabilité dans ASP.NET
- CERTA-2010-AVI-459 : Multiples vulnérabilités dans BIND
- CERTA-2010-AVI-460 : Vulnérabilité dans le noyau Linux

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 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.

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

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 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.

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_rubrique67.html

7 Les bulletins d'actualité

L'objectif des *bulletins d'actualité* est de fournir une illustration par l'actualité récente de certaines mesures de sécurité pragmatiques à appliquer. Bien que par nature *a posteriori*, cette illustration a vocation à servir de base pour tirer des enseignements plus généraux à même de protéger contre des incidents futurs.

L'« actualité » est donnée par l'analyse de machines que le CERTA réalise dans le cadre de ses missions. Un fait est jugé d'actualité, s'il est à la fois récent et significatif, c'est à dire recoupé par différentes analyses.

Les *bulletins d'actualité* n'ont pas la prétention de constituer des statistiques fiables de l'activité informatique malveillante, mais ce qui nous semble avoir beaucoup plus d'intérêt, de montrer à partir d'exemples concrets, réels et anonymisés comment découvrir que l'on est ou a été attaqué et comment limiter l'impact de ces attaques.

La qualité des *bulletins d'actualité* sera améliorée grâce à votre participation. Si vous souhaitez participer, prenez contact avec le CERTA en accord avec votre chaîne fonctionnelle de la sécurité des systèmes d'information.

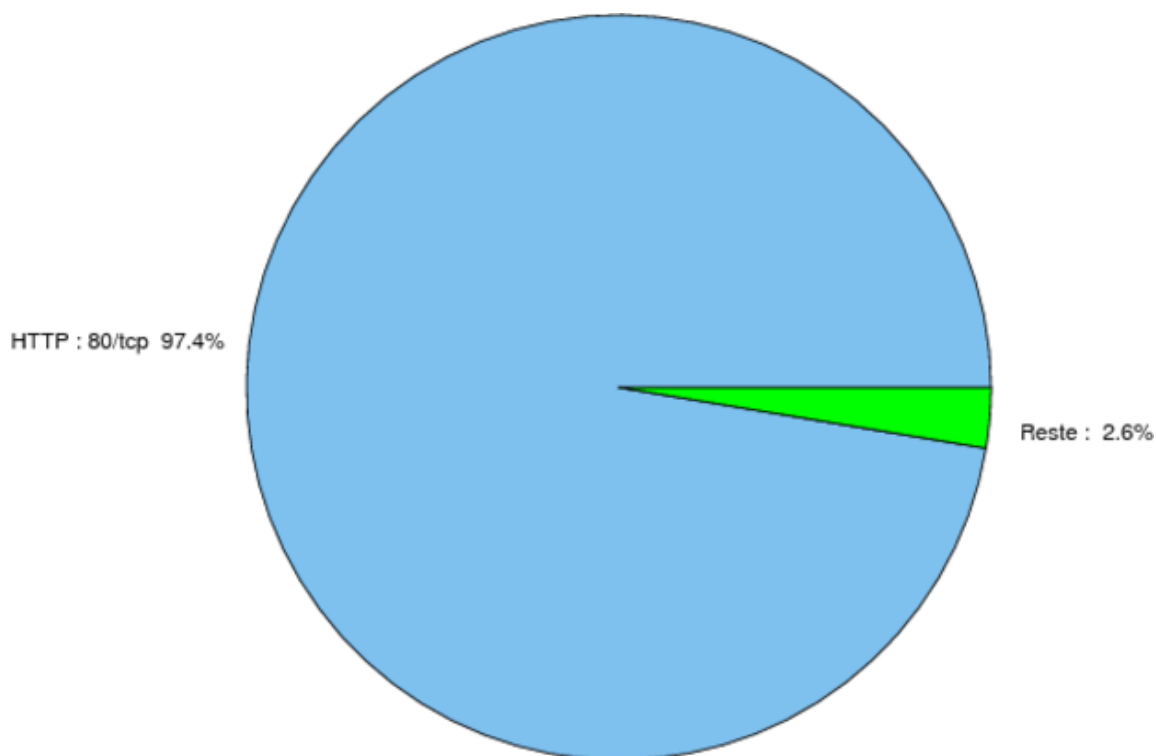


FIG. 1: Répartition relative des ports pour la semaine du 24 au 30 septembre 2010

port	pourcentage
80/tcp	97.43
25/tcp	0.98
445/tcp	0.34
1433/tcp	0.2
2967/tcp	0.19
1080/tcp	0.17
3128/tcp	0.13
23/tcp	0.1
3389/tcp	0.08
135/tcp	0.05
3306/tcp	0.03
4899/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

01 octobre 2010 version initiale.