Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 novembre 2010
N° CERTA-2010-ACT-045

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-45

Gestion du document

Référence	CERTA-2010-ACT-045
Titre	Bulletin d'actualité 2010-45
Date de la première version	12 novembre 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-045.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-045/

1 Vulnérabilité dans Adobe Acrobat Reader

Cette semaine, le CERTA a publié un bulletin d'alerte (CERTA-2010-ALE-020) concernant une vulnérabilité non corrigée dans `Adobe Acrobat Reader`. Celle-ci permet l'exécution de code arbitraire à distance.

Dans l'attente de la publication du correctif par l'éditeur, le CERTA recommande l'application des procédures de contournement provisoire détaillées dans le bulletin d'alerte CERTA-2010-ALE-020.

Documentation

– Alerte CERTA-2010-ALE-020 :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-020

2 Bulletins de sécurité Microsoft

Microsoft a publié cette semaine 3 bulletins de sécurité dont un (MS10-087 `Office`) considéré comme critique. Ils corrigent des vulnérabilités qui peuvent conduire, entre autres, à une exécution de code arbitraire à distance.

Ces mises à jour concernent la suite bureautique MS Office, Powerpoint et Forefront Unified Access Gateway (UAG).

Compte tenu de la criticité de certaines vulnérabilités, le CERTA préconise l'application dans les plus brefs délais des correctifs.

Documentation

- Avis CERTA-2010-AVI-543 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-543
- Avis CERTA-2010-AVI-544 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-544
- Avis CERTA-2010-AVI-545 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-545

3 Incompatibilité de la mise à jour Mac OS X 10.6.5 et PGP WDE

PGP WDE (Whole Disk Encryption) est un outil qui permet le chiffrement complet d'un disque. Cet outil est disponible pour plusieurs systèmes, dont Mac OS X.

Concernant ce dernier, il apparaît que la dernière mise à jour 10.6.5 de Mac OS X n'est pas compatible avec PGP WDE.

L'installation de cette mise à jour, alors que le disque complet est chiffré, peut entraîner une impossibilité de redémarrer le système.

Une solution de contournement est proposée sur le site PGP (cf. Documentation).

Documentation

- Article d'aide PGP du 11 novembre 2010 :
  https://pgp.custhelp.com/app/answers/detail/a_id/2288

4 Problème avec les mises à jour de certains produits Symantec

Certains utilisateurs de produits *Symantec* tels que *Norton Antivirus* ont rencontré des problèmes de mise à jour. Ces désagréments étaient liés à des problèmes de résolution DNS avec certains fournisseurs d'accès. En guise de contournement provisoire, ces utilisateurs pouvaient modifier leur configuration DNS afin de communiquer correctement avec les serveurs de mise à jour.

Ce problème, révélé le 4 novembre 2010, a été corrigé le 11 novembre 2010. Il est donc conseillé, pour tous les utilisateurs de produits *Symantec*, de s'assurer que les dernières mises à jour ont bien été installées. Enfin, pour ceux qui ont modifié leur configuration DNS à cette occasion, une procédure de rétablissement des paramètres par défaut a été proposée par l'éditeur.

Documentation :

- Information sur le forum communautaire de Norton :
  http://fr.community.norton.com/t5/Questions-techniques-sécurité-PC/Mise-à-jour-des-procédures/m-p/3358/highlight/true#M1526
- Procédure de rétablissement des paramètres DNS proposée par l'éditeur :
  http://fr.community.norton.com/t5/Questions-techniques-sécurité-PC/Mise-à-jour-des-procédures/td-p/3340/highlight/true/page/20

5 Sécurisation des ordiphones (*smartphones*)

Les ordiphones (*smartphones*), de la même manière que les stations personnelles, peuvent être la cible de nombreux vecteurs d'attaques souvent ignorés ou mal évalués par les utilisateurs.

5.1 Exemples d'attaques

L'installation d'applications non sécurisées ou malveillantes par l'utilisateur est souvent la cause d'une attaque.

Cette semaine, plusieurs compagnies financières et banques ont mis à jour leurs applications fonctionnant sur Apple iOS et Google Android. En effet, celles-ci gardaient en mémoire des informations d'authentification ou des données personnelles pouvant êtres exploitées ou interceptées par un programme malveillant.

Un autre exemple concerne l'iOS d'Apple. En effet, une publication a été diffusée sur l'Internet démontrant comment, à partir d'une simple page Web, il était possible de passer un appel téléphonique sans avoir à demander la confirmation de l'utilisateur.

Sur le système Android, une démonstration illustre comment un attaquant peut prendre le contrôle à distance du téléphone, là aussi à partir d'une simple page Web. La vulnérabilité utilisée est une faille dans WebKit, composant utilisé dans de nombreux navigateurs tournant sous Android.

Enfin, comme sur les stations de travail, il n'est pas exclus qu'un document spécialement conçu permette à un attaquant d'exécuter du code à distance sur le téléphone.

5.2 Les mises à jour

S'il est possible de récupérer assez facilement des mises à jour concernant les applications, ce n'est pas toujours le cas pour le système d'exploitation fourni avec le téléphone. En effet, si on prend pour exemple le système d'exploitation, il faudra compter sur un nombre important d'intermédiaires avant que la mise à jour atteigne l'utilisateur final (mise à disposition d'un correctif par l'éditeur, intégration par le constructeur du téléphone, puis diffusion par l'opérateur de téléphonie...).

En regardant de plus près la répartition de l'utilisation des différentes versions du système Android de Google (cf. Documentation), on se rend très vite compte qu'un très grand nombre de personnes ne disposent pas de la dernière version du système...

Ce constat doit conduire les responsables des SI à réévaluer les menaces dès lors que des ordiphones peuvent se connecter, légitimement ou non, au SI.

Documentation

- Répartition de l'utilisation des différentes versions du système Android de Google :
  http://developer.android.com/resources/dashboard/platform-versions.html

6 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/

7 Rappel des avis émis

Dans la période du 05 au 11 novembre 2010, le CERTA a émis les avis suivants :

– CERTA-2010-AVI-534 : Vulnérabilités dans MySQL
– CERTA-2010-AVI-535 : Vulnérabilité dans IBM WebSphere
– CERTA-2010-AVI-536 : Multiples Vulnérabilités dans Google Chrome
– CERTA-2010-AVI-537 : Vulnérabilité dans Intel Xeon Baseboard Management Component
– CERTA-2010-AVI-538 : Multiples vulnérabilités dans Adobe Flash Player
– CERTA-2010-AVI-539 : Multiples vulnérabilités dans Cisco Intelligent Contact Manager
– CERTA-2010-AVI-540 : Vulnérabilité dans Cisco Unified Communications Manager
– CERTA-2010-AVI-541 : Vulnérabilités dans Joomla!
– CERTA-2010-AVI-542 : Vulnérabilités dans Novell GroupWise
– CERTA-2010-AVI-543 : Vulnérabilités dans Microsoft Office
– CERTA-2010-AVI-544 : Vulnérabilités dans Microsoft PowerPoint
– CERTA-2010-AVI-545 : Vulnérabilités dans Microsoft Forefront Unified Access Gateway
– CERTA-2010-AVI-546 : Multiples vulnérabilités dans Adobe Flash Server
– CERTA-2010-AVI-547 : Vulnérabilité dans Juniper IVE OS et Netscreen SSL VPN

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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

9 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.

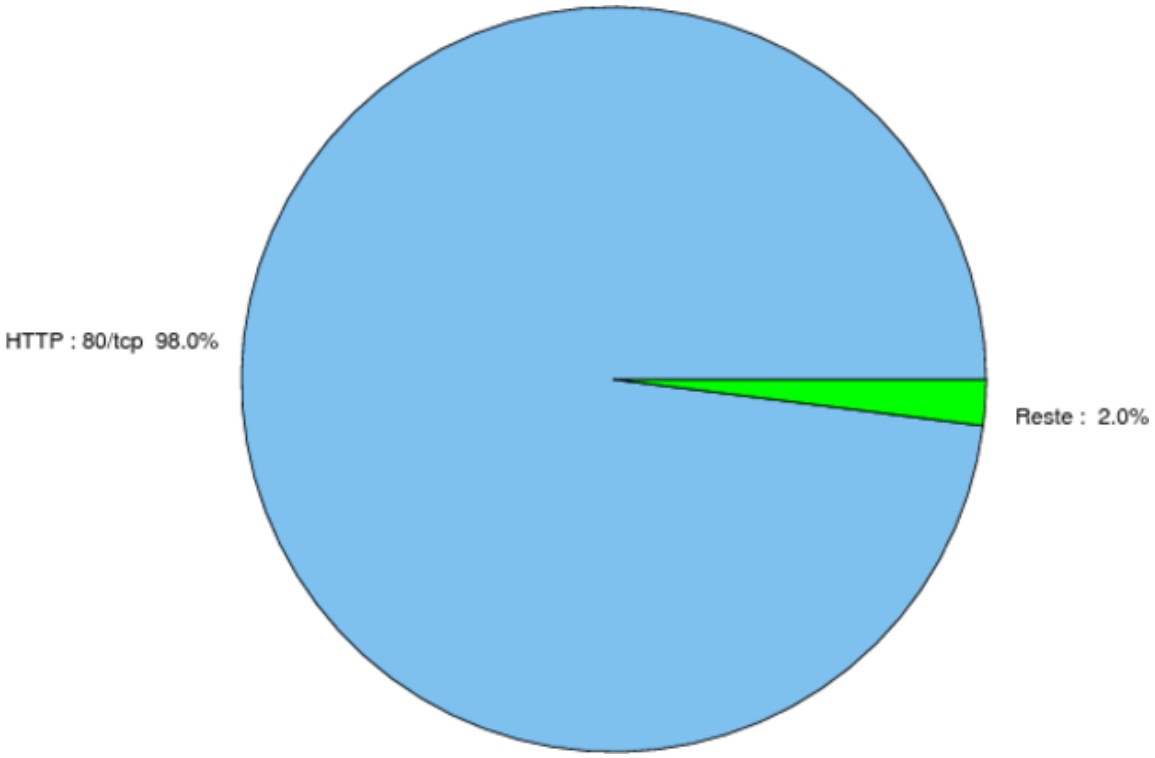

FIG. 1: Répartition relative des ports pour la semaine du 04 au 11 novembre 2010

port	pourcentage
80/tcp	99.32
25/tcp	0.91
2967/tcp	0.24
1080/tcp	0.19
143/tcp	0.15
22/tcp	0.14
445/tcp	0.11
23/tcp	0.06
3389/tcp	0.04
21/tcp	0.03
135/tcp	0.02

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

12 novembre 2010 version initiale.