Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 janvier 2011
N° CERTA-2011-ACT-001

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-01

Gestion du document

Référence	CERTA-2011-ACT-001
Titre	Bulletin d'actualité 2011-01
Date de la première version	07 janvier 2011
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-2011-ACT-001.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-2011-ACT-001/

1 Vulnérabilités de la semaine

1.1 PHP et virgule flottante

Cette semaine, une vulnérabilité importante dans PHP a été corrigée. En effet, sous certaines conditions, le traitement d'une unique valeur en virgule flottante provoquait une boucle infinie entraînant un déni de service. La vulnérabilité intervenait lors de l'initialisation d'une variable avec une valeur représentée par une chaîne de caractères, cette représentation pouvant prendre plusieurs forme pour une même valeur (ex: « 10.2 », « 1.02E01 », « 102E-01 »...). L'exploitation de cette vulnérabilité est triviale, une simple requête de type *GET* peut suffire. Il est précisé sur le site de PHP que seules les plates-formes de type x86 en 32 bits seraient concernées par ce problème.

Le CERTA recommande bien sûr d'effectuer les mises à jour, en respect avec les processus de déploiement locaux.

Documentation

– Notes de mise à jour PHP :
http://www.php.net/archive/2011.php

– Avis CERTA-2011-AVI-003 à propos de PHP du 07 janvier 2011:
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-003/index.html

1.2 Rendu graphique des miniatures dans Windows

Cette semaine le CERTA a publié sa première alerte de l'année, CERTA-2011-ALE-001, à propos d'une vulnérabilité lors du rendu graphique des miniatures dans Windows. Elle concerne les systèmes Windows XP SP2/SP3, Windows Server 2003 SP2, Windows Vista SP1/SP2 et Windows Server 2008 SP2. Microsoft recommande comme moyen de contournement provisoire de limiter les droits de la bibliothèque en charge du rendu (CF. Alertes CERTA et Microsoft). Des exemples de code d'exploitation de cette vulnérabilité sont d'ores et déjà recensés sur l'Internet.

Microsoft précise que cette vulnérabilité, ainsi que celle du 23 décembre 2010 (CERTA-2010-ALE-021) concernant Internet Explorer, ne seront pas corrigées avec les mises à jour du mois de janvier.

Le CERTA recommande l'application, si possible, des moyens de contournements, le respect des bonnes pratiques en matière de SSI, et au besoin, l'utilisation de logiciels alternatifs.

Documentation

– Alerte CERTA-2010-ALE-021 du 23 décembre 2010:
http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-023/index.html
– Alerte CERTA-2011-ALE-001 du 05 janvier 2011:
http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-001/index.html
– Pré annonce des correctifs Microsoft pour le mois de janvier :
http://blogs.technet.com/b/msrc/archive/2011/01/06/advance-notification-service-for-the-january-2011-security-bulletin-release.aspx

2 Contournement des sandbox de sécurité dans Flash Player

`Flash Player` utilise un mécanisme de bac à sable (*sandbox*) afin de cloisonner les interactions entre les fichiers locaux et le réseau. Ce mécanisme n'est pas à confondre avec la sandbox du plugin flash dans chrome évoqué dans *CERTA-2010-ACT-048*.

`Flash Player` assigne les fichiers SWF (`ShockWave Flash`) à des *sandbox* de sécurité différentes, selon leur origine. Les fichiers consultés depuis l'Internet sont ainsi assignés à des *sandbox* séparées correspondantes à leurs sites Web d'origine. Ces fichiers ne sont pas autorisés à charger des ressources ou fichiers locaux.

Les fichiers SWF locaux sont, quant à eux, par défaut placés dans la *sandbox local-with-file-system*. Ils sont alors autorisés à lire des fichiers locaux mais ne peuvent pas communiquer avec le réseau. Cette politique de sécurité est mise en place afin d'éviter qu'un fichier SWF malveillant soit utilisé pour faire de l'exfiltration de documents.

Un chercheur a découvert un moyen contourner cette restriction en permettant à un fichier, assigné à la *sandbox local-with-file-system*, d'envoyer des données sur le réseau. La prévention de l'accès au réseau est réalisée par un mécanisme de liste noire de gestionnaires de protocoles. En utilisant le gestionnaire de protocole *MHTML* qui n'est pas dans cette liste la prévention est contournée et des fichiers peuvent être envoyés sur le réseau. Ce gestionnaire de protocole est présent par défaut sous `Windows 7`.

Le CERTA rappelle que les différentes protections misent en place par cette technologie (*blasklist*, *sandbox*...), restent contournables et ne sont que des éléments constitutifs d'une défense en profondeur du SI.

2.1 Documentation

– Les différentes `sandbox` de sécurité dans `Flash Player`
http://help.adobe.com/en_US/ActionScript/3.0_ProgrammingAS3/WS5b3ccc516d4fbf351e63e3d118a9b90204-7e3f.html

3 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/

4 Rappel des avis émis

Dans la période du 31 décembre 2010 au 06 janvier 2011, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-638 : Multiples vulnérabilités dans WordPress
- CERTA-2010-AVI-639 : Vulnérabilité dans VLC Media Player
- CERTA-2011-AVI-001 : Vulnérabilité dans Wireshark
- CERTA-2011-AVI-002 : Vulnérabilité dans HP Photo Creative

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2010-AVI-612-001 : Vulnérabilités dans MantisBT (ajout des références aux bulletins Fedora et aux CVE)

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

6 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.

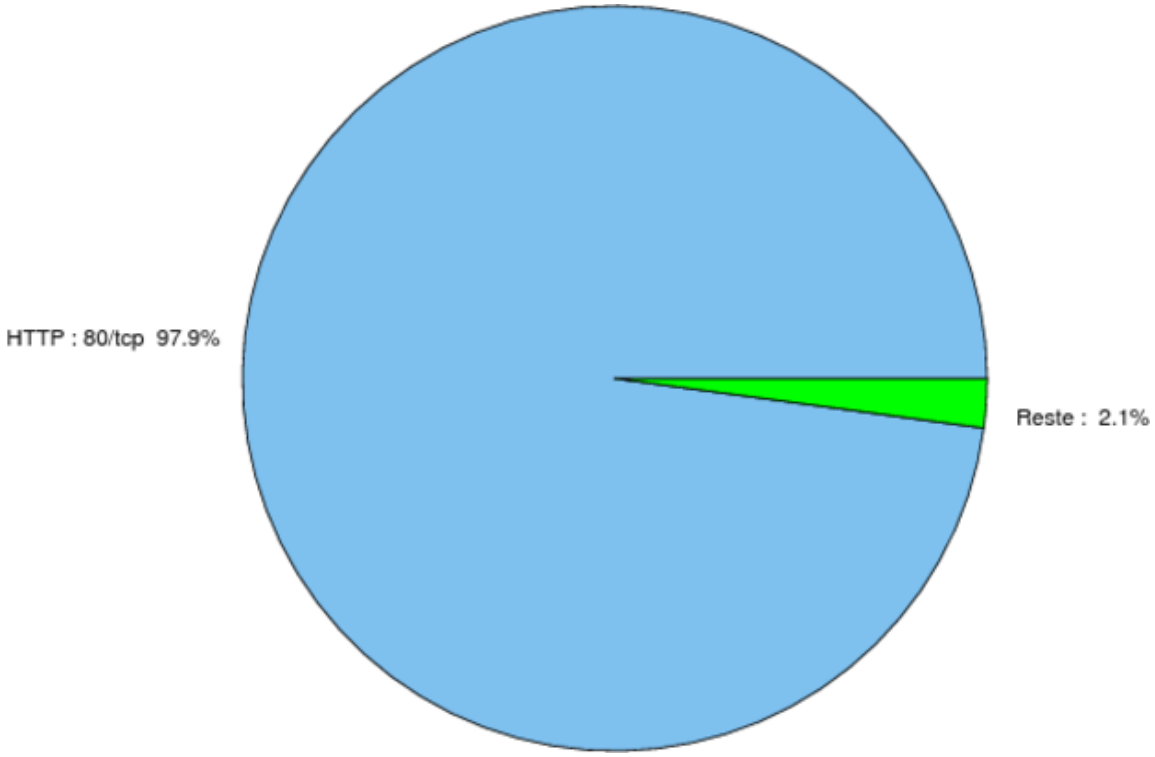

FIG. 1: Répartition relative des ports pour la semaine du 31 décembre 2010 au 06 janvier 2011

port	pourcentage
80/tcp	98.03
25/tcp	0.96
1433/tcp	0.32
445/tcp	0.16
22/tcp	0.11
2967/tcp	0.1
3389/tcp	0.09
23/tcp	0.08
1080/tcp	0.07
135/tcp	0.06
3306/tcp	0.04
4899/tcp	0.02
3128/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

07 janvier 2011 version initiale.