Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 février 2011
N° CERTA-2011-ACT-006

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-06

Gestion du document

Référence	CERTA-2011-ACT-006
Titre	Bulletin d'actualité 2011-06
Date de la première version	11 février 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-006.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-006/

1 Les mises à jour de la semaine

La semaine a été riche en publications de mises à jour par les éditeurs d'application, le CERTA revient sur certains éléments importants.

1.1 Alerte concernant l'environnement d'exécution Java

Cette semaine, Oracle a publié une alerte concernant une vulnérabilité, référencée CVE-2010-4476. Cette dernière permet à une personne distante malintentionnée de provoquer un déni de service du composant JRE (Java Runtime Environment) d'Oracle Java SE et Java for Business Products. Oracle attire l'attention sur l'exposition des applications Java et des serveurs web basés sur cette technologie. Le détail des produits concernés est le suivant :

- Java SE, JDK et JRE 6 mise à jour 23 et versions antérieures pour Windows, Solaris et Linux ;
- Java SE, JDK 5.0 mise à jour 27 et versions antérieures pour Solaris 9 ;
- Java SE, SDK 1.4.2_29 et versions antérieures pour Solaris 8 ;
- Java for Business, JDK et JRE 6 mise à jour 23 et versions antérieures pour Windows Solaris et Linux ;
- Java for Business, JDK et JRE 5.0 mise à jour 27 et versions antérieures pour Windows Solaris et Linux ;

– Java for Business, SDK et JRE 1.4.2_29 et versions antérieures pour Windows Solaris et Linux.

Le CERTA a publié l'avis CERTA-2011-AVI-079 pour cette vulnérabilité. Un correctif, non déployé par le système de mise à jour automatique, est disponible et doit être installé dans les plus brefs délais.

Documentation

– Avis du CERTA CERTA-2011-AVI-079 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-079
– Page de téléchargement du correctif Oracle :
http://www.oracle.com/technetwork/java/javase/downloads/index.html#fpupdater

1.2 Mises à jour Microsoft du mois de février

Microsoft a publié cette semaine douze bulletins de sécurité. Parmi eux, deux bulletins corrigent des alertes CERTA (CERTA-2010-ALE-021 et CERTA-2011-ALE-001). Elles concernent une vulnérabilité dans Internet Explorer et une vulnérabilité dans le moteur de rendu graphique de Windows.

Au total, cinq bulletins corrigent des vulnérabilités permettant d'exécuter du code arbitraire à distance.

Incompatibilités rencontrées dans les mises à jour

Certaines de ces mises à jour nécessitent une attention particulière lors de leur déploiement.

En effet, afin de pouvoir installer le correctif publié dans le bulletin MS11-006 (avis CERTA-2011-AVI-061), il est impératif de supprimer au préalable les mesures de contournement provisoire.

D'autre part, un conflit est apparu entre VMware View Client et l'installation des mises à jour MS11-003 et/ou KB2467023 sur Windows 7. VMware a publié un article et proposé une mise à jour de View Client (version 4.5.0-353760) afin de corriger le problème.

Le CERTA recommande d'appliquer les mises à jour de sécurité dès que possible. Cependant, il est conseillé de procéder à une validation avant de les appliquer sur un système en production.

Documentation

– Base de connaissances VMware KB1034262 du 08 février 2011 :
http://kb.vmware.com/kb/1034262
– Bulletin de sécurité Microsoft MS11-003 du 08 février 2011 :
http://www.microsoft.com/france/technet/security/Bulletin/MS11-003.mspx
http://www.microsoft.com/technet/security/Bulletin/MS11-003.mspx
– Document du CERTA CERTA-2011-AVI-058 du 09 février 2011 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-058/index.html
– Base de connaissances Microsoft KB2467023 du 08 février 2011 :
http://support.microsoft.com/kb/2467023
– Bulletin de sécurité Microsoft MS11-006 du 08 février 2011 :
http://www.microsoft.com/france/technet/security/Bulletin/MS11-006.mspx
http://www.microsoft.com/technet/security/Bulletin/MS11-006.mspx
– Document du CERTA CERTA-2011-AVI-061 du 10 février 2011 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-061/index.html

1.3 Mises à jour Adobe

Cette semaine, Adobe a publié de nombreuses mises à jour concernant trois de ses produits, Adobe Shockwave, Adobe Acrobat et Adobe Flash. La plupart d'entre elles corrigeant des vulnérabilités qui permettent l'exécution de code arbitraire à distance au moyen de documents spécialement formés, le CERTA recommande vivement l'application des correctifs. Pour ce faire, il suffit de vous reporter aux avis du CERTA correspondants (cf. Documentation).

Toutefois, il est à noter que la mise à jour d'Adobe Reader 9.4.2, préconisée dans l'avis CERTA-2011-AVI-076, concernant les systèmes Unix ne sera disponible que pendant la semaine du 28 février 2011. Il est donc préférable d'utiliser sur ces systèmes d'autres lecteurs de fichiers PDF, non connus comme vulnérables, le temps que la mise à jour soit disponible auprès de l'éditeur.

Documentation

- Avis du CERTA CERTA-2011-AVI-075 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-075/index.html
- Avis du CERTA CERTA-2011-AVI-076 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-076/index.html
- Avis du CERTA CERTA-2011-AVI-077 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-077/index.html
- Bulletin de sécurité Adobe APSB11-03 du 8 février 2011 :
  http://www.adobe.com/support/security/bulletins/apsb11-03.html

2 Nouvelle version de Debian et mise à jour de clefs PGP

Cette semaine, le projet Debian a annoncé la publication de la nouvelle version de son système d'exploitation éponyme (`Debian 6.0 « Squeeze »`).

Par ailleurs, il a été également précisé que les clefs PGP utilisées dans la signature des fichiers de référence des miroirs de paquetages ont été mises à jour. Pour l'instant, seules les signatures des branches *testing* et *unstable* sont concernées ainsi que celles des miroirs des mises à jour de sécurité (*security.debian.org*) et les paquetages de *back-portage* (*backports.debian.org*).

Quant à la version stable actuelle (*Squeeze*) et à la version stable précédente (*Lenny*), leurs signatures seront mises à jour lors du passage à une nouvelle version mineure, 6.0.1 et 5.0.9 par exemple.

Recommandations :

Afin d'anticiper cette future mise à jours, il est possible de vérifier que le paquetage *debian-archive-keyring* est bien installé et à jour.

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 04 au 10 février 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-051 : Vulnérabilité dans HP OpenView Performance Insight
- CERTA-2011-AVI-052 : Vulnérabilité dans les produits BlueCoat
- CERTA-2011-AVI-053 : Multiples vulnérabilités dans Google Chrome
- CERTA-2011-AVI-054 : Vulnérabilité dans les produits TANDBERG
- CERTA-2011-AVI-055 : Vulnérabilité dans IBM Build Forge
- CERTA-2011-AVI-056 : Vulnérabilités dans Apache Subversion
- CERTA-2011-AVI-057 : Vulnérabilité dans Majordomo 2
- CERTA-2011-AVI-058 : Vulnérabilités dans Internet Explorer
- CERTA-2011-AVI-059 : Vulnérabilité dans Microsoft Internet Information Server (IIS)
- CERTA-2011-AVI-060 : Vulnérabilité dans Active Directory
- CERTA-2011-AVI-062 : Vulnérabilité dans le pilote Compact Font Format (CCF) OpenType
- CERTA-2011-AVI-063 : Vulnérabilités dans Microsoft Visio
- CERTA-2011-AVI-064 : Vulnérabilité dans les moteurs de JScript et VBScript
- CERTA-2011-AVI-065 : Vulnérabilité dans le processus CSRSS de Windows
- CERTA-2011-AVI-066 : Vulnérabilité dans le noyau Windows
- CERTA-2011-AVI-067 : Vulnérabiltés dans les pilotes en mode noyau de Windows
- CERTA-2011-AVI-068 : Vulnérabilité de Kerberos dans Microsoft Windows
- CERTA-2011-AVI-069 : Vulnérabilité de LSASS dans Microsoft Windows
- CERTA-2011-AVI-070 : Multiples vulnérabilités dans Google Chrome
- CERTA-2011-AVI-071 : Multiples vulnérabilités dans WordPress
- CERTA-2011-AVI-072 : Vulnérabilité dans MediaWiki
- CERTA-2011-AVI-073 : Vulnérabilité dans OpenSSL
- CERTA-2011-AVI-074 : Vulnérabilités dans Dokeos
- CERTA-2011-AVI-076 : Multiples vulnérabilités dans Adobe Reader et Adobe Acrobat
- CERTA-2011-AVI-077 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2011-AVI-078 : Vulnérabilités dans Kerberos
- CERTA-2011-AVI-079 : Vulnérabilité dans Oracle Java
- CERTA-2011-AVI-080 : Vulnérabilités dans ffmpeg
- CERTA-2011-AVI-081 : Multiples vulnérabilités dans Apache Tomcat
- CERTA-2011-AVI-082 : Vulnérabilité dans IBM Lotus Notes
- CERTA-2011-AVI-083 : Multiples vulnérabilités dans Ruby on Rails
- CERTA-2011-AVI-084 : Vulnérabilité dans RealPlayer

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

- CERTA-2010-AVI-550-002 : Vulnérabilités dans IBM HTTP Server et WebSphere (ajout de WebSphere 7x.)
- CERTA-2011-AVI-061-001 : Vulnérabilité dans le moteur de rendu graphique de Windows (référence à l'alerte et précision sur la suppression des mesures de contournement provisoire)

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.

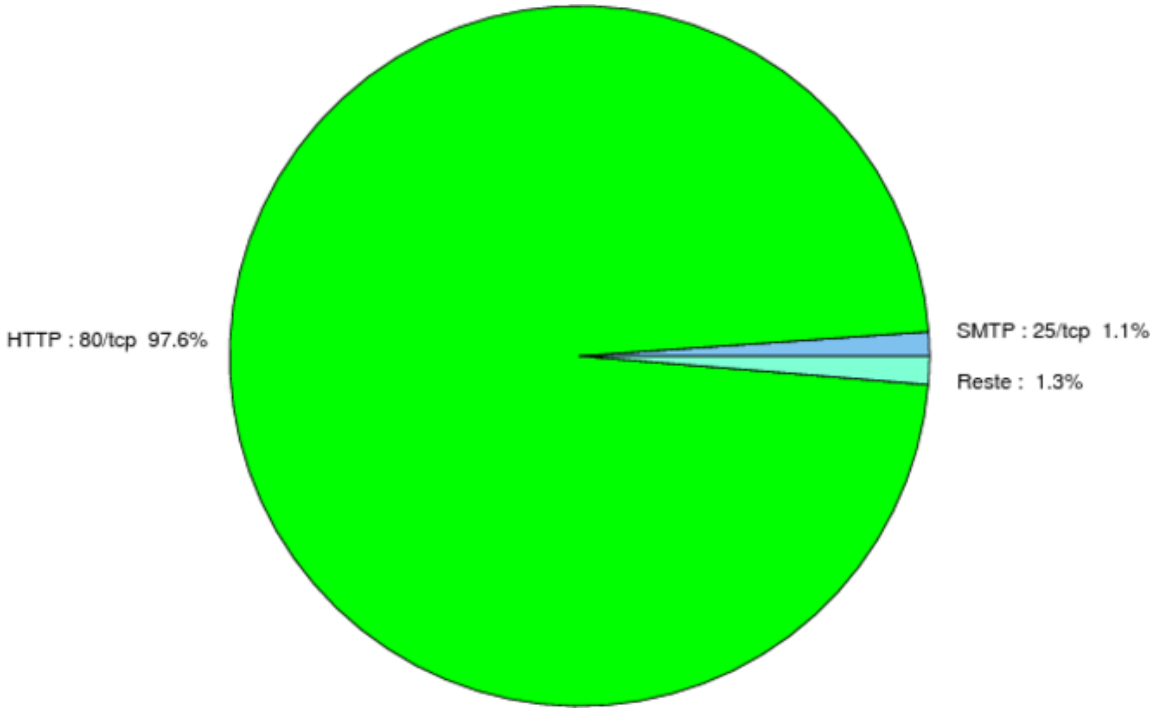

FIG. 1: Répartition relative des ports pour la semaine du 04 au 10 février 2011

port	pourcentage
80/tcp	97.75
25/tcp	1.1
445/tcp	0.34
1080/tcp	0.22
135/tcp	0.16
1433/tcp	0.14
3389/tcp	0.12
23/tcp	0.07
3306/tcp	0.03
4899/tcp	0.02
3128/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

11 février 2011 version initiale.