

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-41

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-041>

Gestion du document

Référence	CERTA-2010-ACT-041
Titre	Bulletin d'actualité 2010-41
Date de la première version	15 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-041.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-041/>

1 Une semaine riche en correctifs

1.1 Mise à jour des produits Microsoft...

Dans son cycle mensuel, Microsoft a publié une longue liste de correctifs répartis dans pas moins de 16 mises à jour différentes. Quatre d'entre elles sont considérées comme critiques par Microsoft (MS10-071, MS10-075, MS10-076, MS10-077, cf. Documentation) et corrigent des vulnérabilités qui peuvent conduire à une exécution de code arbitraire à distance par une personne malintentionnée.

L'ensemble des mises à jour concerne Windows, Internet Explorer, MS .NET Framework en passant par la suite bureautique MS Office et Media Player. Les mises à jour non critiques (mais désignées comme importantes pour la plupart par Microsoft) ne sont pas pour autant à ignorer et doivent également faire l'objet d'une attention particulière.

L'application dans les plus brefs délais de l'ensemble de ces correctifs est impérative.

Documentation

– Avis CERTA-2010-AVI-481

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-481>

- Avis CERTA-2010-AVI-485
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-485>
- Avis CERTA-2010-AVI-486
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-486>
- Avis CERTA-2010-AVI-487
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-487>

1.2 ... et des produits Oracle

Cette semaine, nous retiendrons également deux avis de sécurité importants concernant les produits Oracle. Ceux-ci ciblent des vulnérabilités critiques permettant une exécution de code arbitraire à distance par une personne malintentionnée.

Le premier avis concerne Java SE et Java for Business (CERTA-2010-AVI-500).

Le second avis concerne plusieurs produits Oracle dont Oracle Database, Oracle Application Server, Oracle E-Business Suite ou encore Oracle VM. La liste complète est à consulter sur l'avis CERTA-2010-AVI-499.

Les correctifs publiés sont à appliquer impérativement pour les produits concernés.

Documentation

- Avis CERTA-2010-AVI-499
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-499>
- Avis CERTA-2010-AVI-500
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-500>

2 La CNIL publie un guide de la sécurité des données personnelles

La CNIL vient de publier sur son site un guide pour la sécurité des données personnelles. Après un rappel des contraintes légales qui s'appliquent aux SI, le document présente une série de fiches de conseil par domaine technique et administratif (sécurité des locaux, sécurisation des terminaux mobiles, authentification des utilisateurs, sous-traitance, ...).

Chaque fiche présente les précautions élémentaires à mettre en œuvre, les bonnes pratiques à suivre ainsi que des solutions à éviter. Elles sont également accompagnées de documents « type » (charte informatique, clause de confidentialité en cas de sous-traitance, ...).

Rédigé dans l'état de l'art de la technique et du droit, dépassant souvent le cadre du traitement des données personnelles, il s'agit en pratique d'un document très intéressant aussi bien pour les responsables de grands systèmes d'information que pour les administrateurs de PME.

Le CERTA rappelle qu'il est important de se poser la question de la déclaration de tout fichier de données à caractères personnelles auprès de la CNIL et que des mesures de protection doivent être mise en place afin d'en assurer leur confidentialité.

Documentation

- Le guide de la sécurité des données personnelles :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite%20VD.pdf

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 01 au 07 octobre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-477 : Multiples vulnérabilités dans phpCAS
- CERTA-2010-AVI-478 : Vulnérabilité dans RSA Authentication Client
- CERTA-2010-AVI-480 : Vulnérabilités dans IBM WebSphere
- CERTA-2010-AVI-481 : Vulnérabilités dans Internet Explorer
- CERTA-2010-AVI-482 : Multiples vulnérabilités dans SafeHTML
- CERTA-2010-AVI-483 : Vulnérabilités dans les pilotes en mode noyau de Windows
- CERTA-2010-AVI-484 : Vulnérabilité dans Microsoft Foundation CLasses
- CERTA-2010-AVI-485 : Vulnérabilité dans le service de partage réseau de Media Player
- CERTA-2010-AVI-486 : Vulnérabilité dans le moteur de polices Embedded OpenType de Windows
- CERTA-2010-AVI-487 : Vulnérabilité dans Microsoft NET
- CERTA-2010-AVI-488 : Vulnérabilités dans le pilote de format OpenType Font
- CERTA-2010-AVI-489 : Vulnérabilités dans Microsoft Office Word
- CERTA-2010-AVI-490 : Vulnérabilités dans Microsoft Office Excel
- CERTA-2010-AVI-491 : Vulnérabilité dans Windows Explorer Common Control Library
- CERTA-2010-AVI-492 : Vulnérabilité dans Windows Media Player
- CERTA-2010-AVI-493 : Vulnérabilité dans l'interpréteur Windows et WordPad
- CERTA-2010-AVI-494 : Vulnérabilité dans Windows
- CERTA-2010-AVI-495 : Vulnérabilité dans Microsoft Windows Secure Channel
- CERTA-2010-AVI-496 : Vulnérabilité dans le partage de cluster de disques sous Windows Server
- CERTA-2010-AVI-497 : Vulnérabilité dans Wireshark
- CERTA-2010-AVI-498 : Multiples vulnérabilités dans Opera
- CERTA-2010-AVI-499 : Multiples vulnérabilités dans les produits Oracle
- CERTA-2010-AVI-500 : Multiples vulnérabilités dans Oracle Java

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

- CERTA-2010-AVI-479-001 : Vulnérabilités dans Xpdf (ajout des références aux bulletins de sécurité Red Hat)

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 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.

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 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.

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_rubrique67.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.

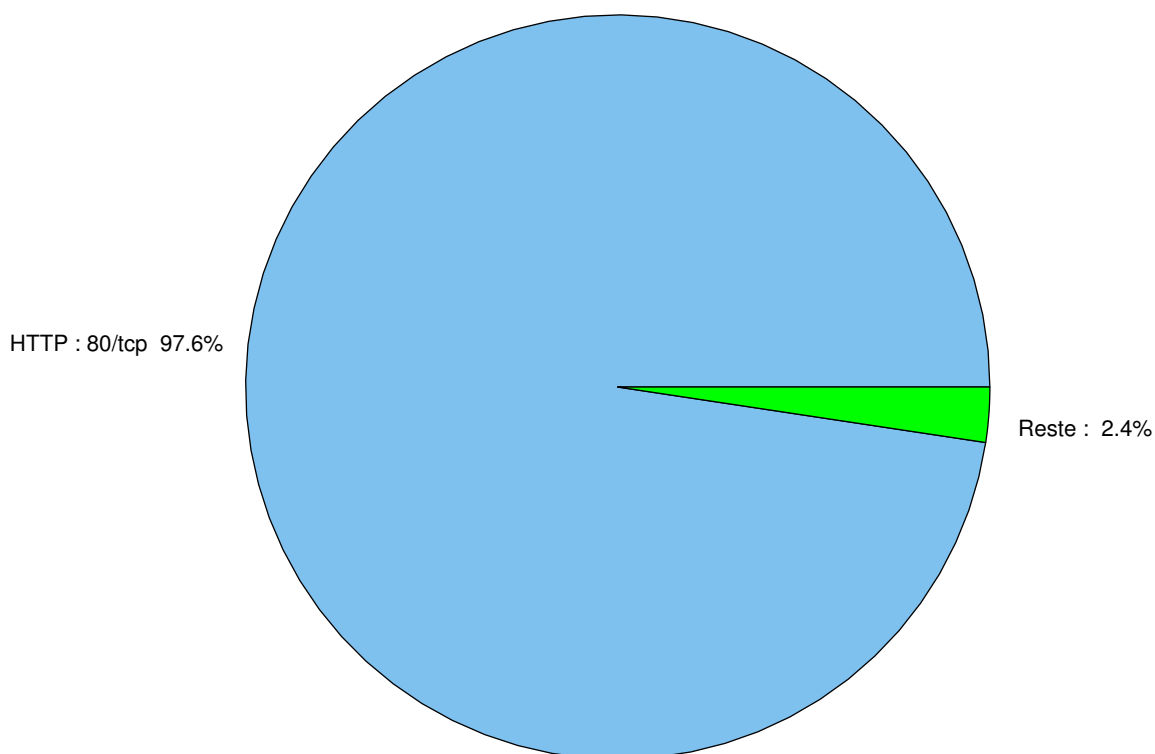


FIG. 1: Répartition relative des ports pour la semaine du 01 au 07 octobre 2010

port	pourcentage
80/tcp	97.67
25/tcp	0.95
1080/tcp	0.3
445/tcp	0.24
3306/tcp	0.2
1433/tcp	0.16
22/tcp	0.14
2967/tcp	0.13
135/tcp	0.05
3128/tcp	0.04
1434/udp	0.03
3389/tcp	0.02

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

15 octobre 2010 version initiale.