

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-50

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-050>

Gestion du document

Référence	CERTA-2010-ACT-050
Titre	Bulletin d'actualité 2010-50
Date de la première version	17 décembre 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-050.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-050/>

1 Mise à jour des produits Microsoft

Comme tous les mois, *Microsoft* a publié cette semaine une liste de correctifs de certains de ses produits, couvrant de nombreuses versions de *Windows*. Parmi les 17 avis émis par *Microsoft*, dix traitent de vulnérabilités permettant l'exécution de code arbitraire à distance.

On pourra également noter que le bulletin de sécurité MS10-090 (voir l'avis CERTA-2010-AVI-593) corrige la vulnérabilité décrite dans l'alerte CERTA-2010-ALE-019 du 03 novembre 2010.

Compte tenu de la criticité des failles corrigées, il est impératif d'appliquer l'ensemble des correctifs de manière diligente.

Documentation

- Avis CERTA-2010-AVI-593 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-593>
- Alerte CERTA-2010-ALE-019 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-019>

2 Dépôt d'une porte dérobée dans phpMyFAQ

Les développeurs du projet *phpMyFAQ* ont annoncé sur leur site Web (<http://www.phpmyfaq.de>) que le serveur principal du projet avait été compromis. Cette attaque a eu pour conséquence le dépôt de versions contenant une porte dérobée. Les versions affectées par cette modification sont *phpMyFAQ* 2.6.11 et 2.6.12. L'attaquant a également changé les fichiers de condensats cryptographiques (hash) MD5 afin de dissimuler la modification des sources.

La porte dérobée a été ajoutée dans le fichier *inc/Faq.php* et encodée en base64. Ce code envoie tout d'abord un courriel vers une adresse définie puis ajoute une entrée dans la table *faqconfig* utilisée par *phpMyFAQ*. Cette entrée est ensuite utilisée comme porte dérobée en permettant d'inclure du code PHP arbitraire.

Les sources contenant cette porte dérobée ont été disponibles en téléchargement du 04 au 15 décembre 2010. Le CERTA recommande, par précaution, à tous les administrateurs ayant déployé *phpMyFAQ* de vérifier les condensats cryptographiques (hash MD5) des sources sur la page de l'éditeur.

Documentation

- Avis CERTA-2010-AVI-616 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-616>
- Bulletin de sécurité phpMyFAQ annonçant la compromission du serveur :
http://www.phpmyfaq.de/advisory_2010-12-15.php
- Fichiers de signature MD5 des sources de phpMyFAQ 2.6.11 et 2.6.12 :
http://www.phpmyfaq.de/download_old.php

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 10 au 16 décembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-585 : Vulnérabilités dans les produits Mozilla
- CERTA-2010-AVI-586 : Multiples vulnérabilités dans RealPlayer
- CERTA-2010-AVI-587 : Vulnérabilités dans Exim 4
- CERTA-2010-AVI-588 : Vulnérabilité dans Lotus Mobile Connect
- CERTA-2010-AVI-589 : Vulnérabilité dans des produits de chiffrement Sophos
- CERTA-2010-AVI-590 : Vulnérabilités dans OpenSSL
- CERTA-2010-AVI-591 : Vulnérabilités dans Novell ZENworks
- CERTA-2010-AVI-592 : Multiples vulnérabilités dans Google Chrome
- CERTA-2010-AVI-593 : Vulnérabilités dans Microsoft Internet Explorer
- CERTA-2010-AVI-594 : Vulnérabilité dans le planificateur de tâches de Windows
- CERTA-2010-AVI-595 : Vulnérabilités dans le pilote de police OpenType
- CERTA-2010-AVI-596 : Vulnérabilité dans Microsoft Movie Maker
- CERTA-2010-AVI-597 : Vulnérabilité dans le codeur Windows Media
- CERTA-2010-AVI-598 : Vulnérabilité dans Windows
- CERTA-2010-AVI-599 : Vulnérabilité dans le carnet d'adresses Windows
- CERTA-2010-AVI-600 : Vulnérabilité dans l'assistant de connexion Internet Windows
- CERTA-2010-AVI-601 : Multiples vulnérabilités dans le sous-système graphique Windows
- CERTA-2010-AVI-602 : Vulnérabilité dans le noyau de Windows
- CERTA-2010-AVI-603 : Vulnérabilité dans l'interface utilisateur Microsoft
- CERTA-2010-AVI-604 : Vulnérabilité dans le service Netlogon de Microsoft Windows
- CERTA-2010-AVI-605 : Vulnérabilité dans Microsoft Windows Hyper-V VMBus
- CERTA-2010-AVI-606 : Vulnérabilités dans Microsoft Publisher
- CERTA-2010-AVI-607 : Vulnérabilité dans Microsoft Office SharePoint Server
- CERTA-2010-AVI-608 : Vulnérabilités dans Microsoft Office
- CERTA-2010-AVI-609 : Vulnérabilité dans Microsoft Exchange Server
- CERTA-2010-AVI-610 : Vulnérabilité dans BlackBerry Enterprise Server
- CERTA-2010-AVI-611 : Vulnérabilité dans des produits TIBCO
- CERTA-2010-AVI-612 : Vulnérabilités dans MantisBT
- CERTA-2010-AVI-613 : Vulnérabilité dans les produits F-Secure

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

- CERTA-2010-AVI-576-001 : Vulnérabilités dans ClamAV (ajout des références aux bulletins Fedora, Mandriva et Ubuntu, et des 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 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.

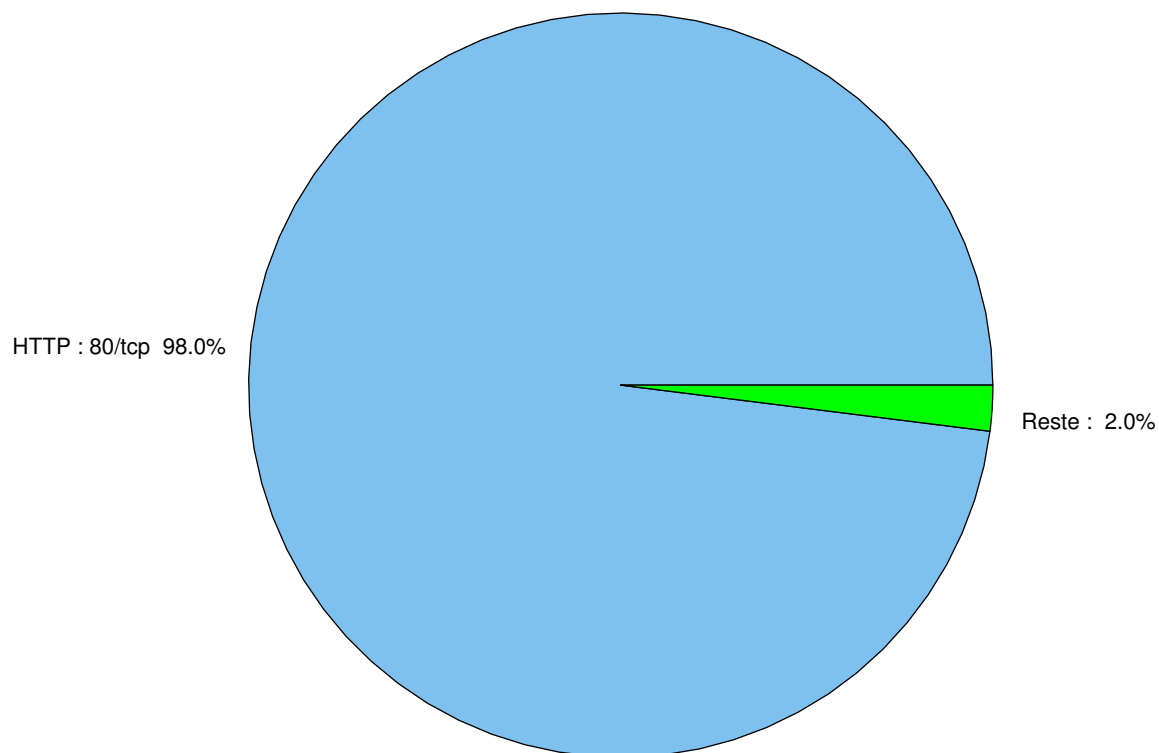


FIG. 1: Répartition relative des ports pour la semaine du 10 au 16 décembre 2010

port	pourcentage
80/tcp	98.28
25/tcp	0.84
1080/tcp	0.19
1433/tcp	0.17
23/tcp	0.14
22/tcp	0.12
3389/tcp	0.08
135/tcp	0.04
3127/tcp	0.03
3128/tcp	0.02
3306/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

17 décembre 2010 version initiale.