

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-02

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-2011-ACT-002>

Gestion du document

Référence	CERTA-2011-ACT-002
Titre	Bulletin d'actualité 2011-02
Date de la première version	14 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-002.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-002/>

1 Compromission d'un serveur Web

Cette semaine, le CERTA a traité le cas d'un serveur Web compromis, impliqué dans une attaque en déni de service. L'analyse de cette machine a permis de mettre en évidence l'exploitation d'une faille de *phpMyAdmin* connue depuis mars 2009 (voir avis CERTA-2010-AVI-117). Le principe de cette faille consiste à effectuer une opération de sauvegarde de nouvelle configuration, cette dernière correspondant en réalité à du code PHP exécutable. Une telle attaque laisse des traces significatives dans les journaux, par exemple :

```
<IP attaquant> - - [13/01/2011:20:18:51 +0100] "POST /phpmyadmin/scripts/setup.php  
HTTP/1.1" 200 284789 "Opera"
```

L'attaquant a par la suite installé divers outils dans le répertoire `/var/tmp/" "` (le nom du sous-répertoire n'est composé que d'un seul « espace »).

Le serveur ainsi compromis a été utilisé comme robot IRC. Il recevait des instructions d'attaque (déni de service ou exploitation de vulnérabilités) au travers d'un canal IRC.

La lecture des journaux du serveur indique que celui-ci était régulièrement compromis par cette faille de *phpMyAdmin*.

Les incidents de ce type ne sont pas isolés. C'est la raison pour laquelle le CERTA recommande d'entreprendre les actions suivantes :

- mettre à jour systématiquement les logiciels utilisés. L'application du correctif de *phpMyAdmin* dès sa publication aurait empêché la compromission du serveur ;
- filtrer les connexions sortantes du serveur. Dans notre cas, un filtrage des connexions vers des serveurs IRC aurait fortement limité l'impact de la compromission ;
- lire les journaux, et rechercher notamment les requêtes POST réussies sur le fichier `setup.php` ;
- vérifier régulièrement le contenu du répertoire `/var/tmp` car les intrus y déposent souvent une partie de leurs outils (ce n'est pas systématique).

Documentation :

- Avis CERTA-2009-AVI-117 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2009-AVI-117/>

2 Mises à jour Microsoft du mois de janvier

Cette semaine, Microsoft a publié deux bulletins de sécurité dans le cadre de ses mises à jour mensuelles.

Le premier bulletin concerne une vulnérabilité dans le gestionnaire de sauvegarde de Windows Vista et permet à une personne malveillante d'exécuter du code arbitraire à distance. Le deuxième bulletin concerne deux vulnérabilités et tous les systèmes Microsoft Windows. Leur exploitation permet l'exécution de code arbitraire au moyen d'une page web spécialement conçue.

Cette semaine, le CERTA a également mis à jour l'alerte CERTA-2010-ALE-021 sur Internet Explorer qui n'a pas été corrigée par le lot de correctifs de janvier. Un contournement provisoire a en revanche été publié par Microsoft. Celui-ci modifie la bibliothèque `MSHTML.DLL` et il est impératif d'avoir auparavant installé la mise à jour MS10-090 du 14 décembre 2010. L'application de ce contournement est fortement recommandée, toutefois la prudence s'impose quant aux éventuels effets de bord.

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 07 au 13 janvier 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-003 : Vulnérabilité dans PHP
- CERTA-2011-AVI-004 : Vulnérabilités dans les paquetages tiers pour VMware
- CERTA-2011-AVI-005 : Multiples vulnérabilités dans evince
- CERTA-2011-AVI-006 : Vulnérabilité dans Mac OS X
- CERTA-2011-AVI-007 : Vulnérabilité dans Mono
- CERTA-2011-AVI-008 : Vulnérabilité dans Novell Identity Manager
- CERTA-2011-AVI-009 : Vulnérabilité dans Windows Vista
- CERTA-2011-AVI-010 : Vulnérabilités dans Microsoft Data Access Components
- CERTA-2011-AVI-011 : Vulnérabilité dans Struts
- CERTA-2011-AVI-012 : Vulnérabilité dans Symantec Web Gateway

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

- CERTA-2010-AVI-635-001 : Vulnérabilités dans Django (ajout des références au bulletin Ubuntu et aux CVE)
- CERTA-2011-AVI-005-001 : Multiples vulnérabilités dans evince (ajout du correctif Fedora)

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_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.

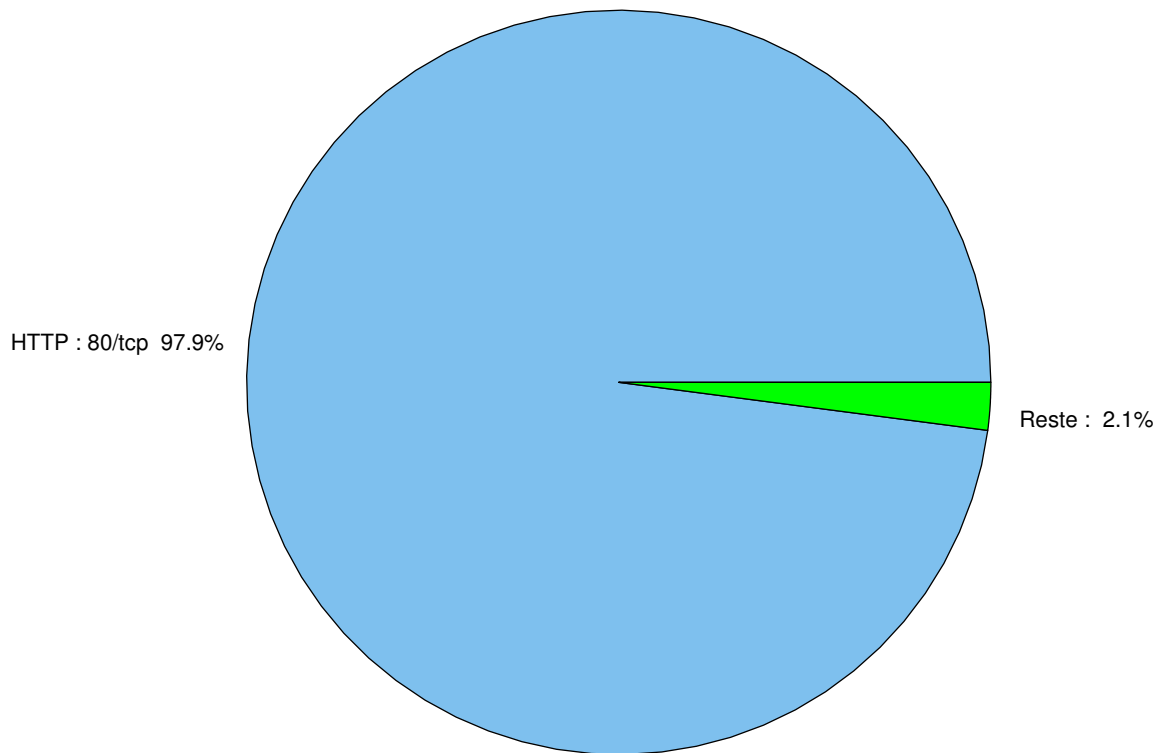


FIG. 1: Répartition relative des ports pour la semaine du 07 au 13 janvier 2011

port	pourcentage
80/tcp	98.01
25/tcp	0.8
1433/tcp	0.29
3306/tcp	0.23
23/tcp	0.16
445/tcp	0.15
22/tcp	0.13
3389/tcp	0.09
135/tcp	0.08
3128/tcp	0.02
1080/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	5

Gestion détaillée du document

14 janvier 2011 version initiale.