

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2011-08**

---

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-008>

---

### Gestion du document

Référence	CERTA-2011-ACT-008
Titre	Bulletin d'actualité 2011-08
Date de la première version	25 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-008.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-008/>

## 1 Exploitation de vulnérabilités d'équipements réseau

### 1.1 Attaque et conséquences

Cette semaine, le CERTA a été avisé de l'exploitation active d'un double défaut de configuration de boîtier ADSL (*box*) d'une gamme particulière.

Quand l'attaquant parvient à exploiter ces vulnérabilités, il devient capable de modifier la configuration réseau de l'équipement. Dans les nombreux cas observés par l'opérateur, les DNS primaire et secondaire inscrits dans l'équipement étaient modifiés. L'utilisateur abonné de l'opérateur n'interrogeait plus les DNS de son opérateur, mais les serveurs frauduleusement mis dans la configuration.

L'impact de cette simple modification n'est pas négligeable. Dès que le DNS auquel l'utilisateur s'adresse, sans le savoir, est malveillant, beaucoup de manipulations sont possibles de la part des attaquants :

- analyse du trafic de l'utilisateur ;
- capture de données personnelles, d'informations de connexion ou de données bancaires ;
- détournement des courriels ;
- déroutement vers des sites Web injectant des programmes malveillants ;
- etc.

Pour mémoire, la modification de la configuration DNS dans les ordinateurs eux-mêmes est la méthode utilisée par la famille de programmes malveillants appelés justement *DNSChanger*, répandus dès 2007.

## 1.2 Recommandations

Pour ces équipements, le CERTA recommande une configuration basée sur le principe de défense en profondeur, même si les modalités de déploiement sont particulières pour cette gamme d'équipements :

- maintien à jour des systèmes d'exploitation des logiciels et des greffons ;
- suppression des services inutiles (désactivation, voire désinstallation) ;
- restriction d'accès sur les différentes interfaces réseau ;
- utilisation de mots de passe robustes et, chaque fois que cela est possible, à durée de vie limitée ;
- journalisation des événements, dont les changements de modification, et analyse de ces journaux ;
- contrôles réguliers, par exemple confrontation périodique de la configuration implantée et de la configuration théorique.

## 2 Service Pack 1 pour Windows 7 et Windows Server 2008 R2

Depuis peu, un premier *service pack* est disponible pour Windows 7 et Windows 2008 R2. Celui-ci est publié sur le site de Microsoft mais aussi dans Windows Update.

Le *service pack* 1 n'apporte pas de fonctionnalité majeure mais un grand nombre de correctifs. Ainsi, il comporte 39 mises à jour de sécurité et plus de 750 *hotfixes*. Ces derniers ne sont en général pas téléchargés automatiquement et apportent des améliorations de performance et/ou de stabilité. La liste complète est disponible sur le site de l'éditeur.

Parmi les nouveautés, Microsoft annonce surtout quelques nouvelles fonctionnalités pour Windows Server 2008 R2 (allocation dynamique de mémoire pour Hyper-V, *RemoteFX*, améliorations de *DirectAccess*, etc.).

Le CERTA recommande la plus grande prudence pour l'installation du service pack 1, cela pouvant en effet causer des effets de bord. Il est recommandé d'attendre quelques jours voire semaines et de procéder à une recette avant de le déployer massivement sur un parc entier d'ordinateurs ou sur un système critique.

### Documentation

- Documentation sur le service pack :  
<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=61924cea-83fe-46e9-96d8-027ae59ddc11>

## 3 Vulnérabilité du noyau Linux

Cette semaine, deux CVE relatifs à des vulnérabilités dans le noyau Linux ont été publiés : CVE-2011-1011 et CVE-2011-1012. Le premier concerne une vulnérabilité liée au support des partitions de type MAC que l'on trouve de façon très classique avec les systèmes de type Mac OS X. Un utilisateur malintentionné peut causer un arrêt inopiné du système par le biais de l'insertion d'un support de données (disque dur ou une clef USB) présentant une table de partitions MAC particulière. La seconde vulnérabilité, quant à elle, est relative au support des partitions de type Microsoft Logical Volume Manager (LDM) et permet à un utilisateur malintentionné de provoquer un arrêt inopiné du système, ou bien encore d'élever ses privilèges (accès au système sans authentification) en insérant sur la machine vulnérable un support de données présentant une table de partitions LDM particulière.

### Recommandation :

En attendant que des correctifs soient proposés dans les noyaux des distributions GNU/Linux ou dans les sources du noyau standard (<http://kernel.org>), il est recommandé de ne pas insérer de support amovible utilisant ces types de partitionnement. Il est aussi possible de recompiler les sources pour obtenir un noyau ne disposant pas du support pour ces partitionnements.

## 4 Prise en compte d'IPv6 dans Debian Squeeze

Dans la dernière version stable de la distribution GNU/Linux Debian, l'intégration du protocole IPv6 ne se présente plus, comme dans les anciennes versions de Debian sous la forme de modules du noyau. En effet, la mise en œuvre d'IPv6 est maintenant incluse dans le noyau directement. Il n'est donc plus possible de télécharger le ou les modules *ad-hoc* pour désactiver le support du protocole.

Dans la plupart des cas, IPv6, bien que présent, n'est pas utilisé et augmente de façon inutile la surface d'attaque du système (cf. <http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-004/index.html>). Il conviendra donc de le désactiver soit en recompilant un noyau sans le support de IPv6 soit par le biais de contrôles système particuliers (*sysctl*) en positionnant dans le fichier */etc/sysctl.conf* les variables suivantes :

```
# désactivation du support pour les interfaces actuelles
net.ipv6.conf.all.disable_ipv6 = 1

# désactivation du support de l'autoconfiguration
net.ipv6.conf.all.autoconf = 0

# désactivation du support par défaut pour les nouvelles interfaces
net.ipv6.conf.default.disable_ipv6 = 1

# désactivation du support pour l'interface de bouclage
net.ipv6.conf.lo.disable_ipv6 = 1
```

Il est à noter que le fait de positionner ces variables dans le fichier ne suffit pas. Il faudra, soit, de façon cavalière, redémarrer la machine soit, de façon plus intelligente, utiliser la commande *sysctl* comme suit :

```
sysctl -w net.ipv6.conf.all.disable_ipv6=1
sysctl -w net.ipv6.conf.all.autoconf=0
sysctl -w net.ipv6.conf.default.disable_ipv6=1
sysctl -w net.ipv6.conf.lo.disable_ipv6=1
```

## 5 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/>

## 6 Rappel des avis émis

Dans la période du 18 au 24 février 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-096 : Vulnérabilité dans Novell ZENworks Configuration Management
- CERTA-2011-AVI-097 : Vulnérabilité dans ClamAV
- CERTA-2011-AVI-098 : Multiples vulnérabilités dans Asterisk
- CERTA-2011-AVI-099 : Vulnérabilité dans IBM FileNet Content Manager
- CERTA-2011-AVI-100 : Vulnérabilités dans Mailman
- CERTA-2011-AVI-101 : Multiples vulnérabilités dans Ruby
- CERTA-2011-AVI-102 : Vulnérabilités dans RedHat Directory Server
- CERTA-2011-AVI-103 : Vulnérabilité dans ISC Bind
- CERTA-2011-AVI-104 : Vulnérabilité dans Cisco Firewall Services Module
- CERTA-2011-AVI-105 : Multiples vulnérabilités dans les logiciels Cisco TelePresence
- CERTA-2011-AVI-106 : Vulnérabilité dans CA HIPS
- CERTA-2011-AVI-107 : Vulnérabilité dans Novell Netware
- CERTA-2011-AVI-108 : Vulnérabilité dans Microsoft Malware Protection Engine
- CERTA-2011-AVI-109 : Multiples vulnérabilités dans Cisco ASA série 5500
- CERTA-2011-AVI-110 : Vulnérabilité dans IBM WepSphere Portal

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

- CERTA-2011-AVI-079-003 : Vulnérabilité dans plusieurs implémentations de Java (ajout des références au bulletin de sécurité IBM CICS)

## 7 Actions suggérées

### 7.1 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.

### 7.2 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.

### 7.3 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.

## 7.4 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.

## 7.5 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.

## 7.6 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.

## 7.7 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](http://www.ssi.gouv.fr/site_rubrique62.html)

# 8 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.

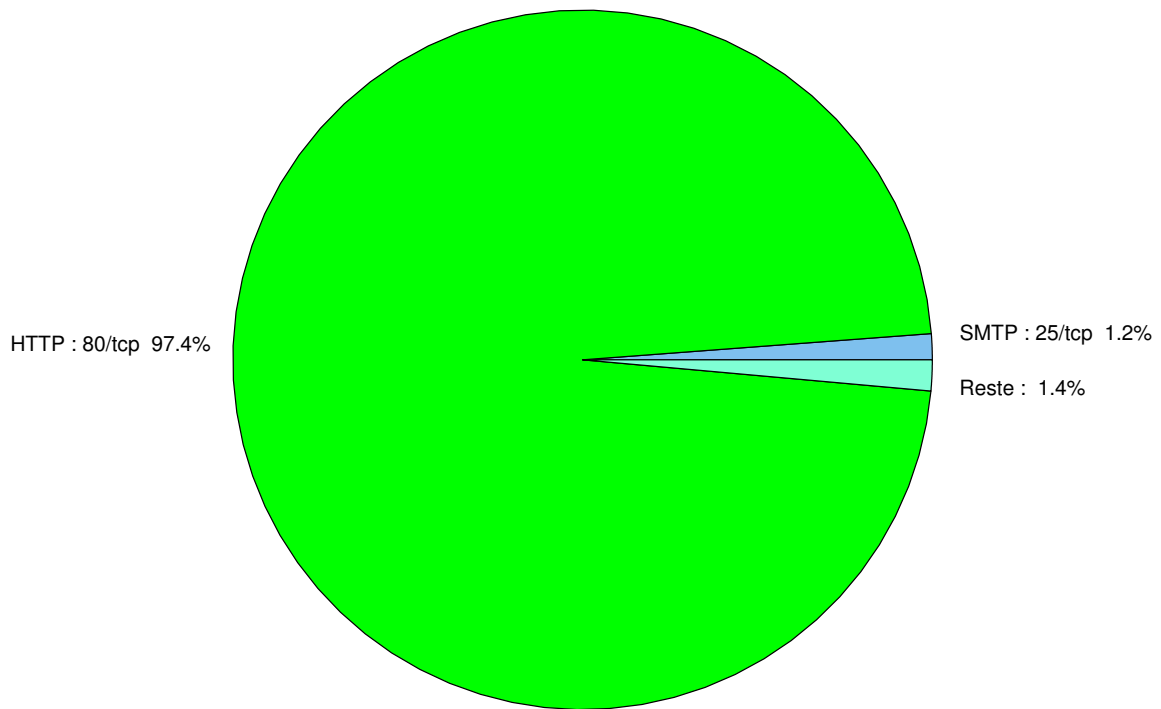


FIG. 1: Répartition relative des ports pour la semaine du 18 au 24 février 2011

port	pourcentage
80/tcp	97.44
25/tcp	1.19
445/tcp	0.45
1433/tcp	0.25
1080/tcp	0.19
22/tcp	0.18
3389/tcp	0.14
23/tcp	0.06
135/tcp	0.04
3306/tcp	0.02
1434/udp	0.01

TAB. 2: Paquets rejetés

## Liste des tableaux

1	Gestion du document . . . . .	1
2	Paquets rejetés . . . . .	6

## Gestion détaillée du document

25 février 2011 version initiale.