Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 janvier 2011
N° CERTA-2011-ACT-003

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité 2011-03**

| | |
|---|---|
| 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-003` |

## Gestion du document

| | |
|---|---|
| Référence | CERTA-2011-ACT-003 |
| Titre | Bulletin d'actualité 2011-03 |
| Date de la première version | 21 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-003.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-003/

## 1 Une version officieuse du SP1 de Windows 7 disponible ?

Un an environ après la sortie de *Microsoft Windows 7*, de nombreux utilisateurs attendent la sortie du Service Pack 1 (SP1) pour ce système, qui apportera des correctifs améliorant le système de virtualisation, certains composants graphiques, la stabilité et la sécurité du système, ainsi que de nouvelles fonctionnalités.

La version « Release Candidate » de ce Service Pack est déjà disponible depuis le mois d'octobre. Mais selon l'équipe russe de Microsoft travaillant sur les fonctionnalités de virtualisation, la version « Release To Manufacturing », celle qui sera gravée sur CDROM en usine pour commercialisation, est d'ores et déjà prête. Il ne s'agit en revanche pas encore de la version qui sera distribuée au public. La mise à disposition de ce Service Pack au grand public est annoncée sur le bloc-notes de l'équipe technique de Microsoft pour le premier trimestre 2011. Toutefois la version RTM est actuellement distribuée sur l'Internet.

Bien qu'il paraît raisonnable de penser qu'aucune modification ne sera apportée à la version RTM avant sa mise à disposition auprès du public, le CERTA déconseille fortement l'installation de mises à jour lorsque celles-ci ne sont pas directement et officiellement fournies par l'éditeur. Il n'y a en effet aucun moyen de s'assurer de leur innocuité.

## Documentation

- Bloc-notes de l'équipe de développement Windows :
  http://windowsteamblog.com/windows/b/business/archive/2010/11/03/windows-7-momentum-and-customer-guidance.aspx
- Bloc-notes sur la virtualisation dans Windows :
  http://blogs.technet.com/b/vm/archive/2011/01/14/service-pack-1-windows-7-windows-server-2008-r2.aspx

# 2 Vulnérabilité critique dans SPIP

Le CERTA a publié cette semaine un avis (CERTA-2011-AVI-018) concernant une faille critique découverte dans *SPIP*. Cette vulnérabilité affecte les versions 2.0.x et 2.1.x du logiciel et permet de détruire des fichiers du site, ainsi que la base de données. Il est à noter que des utilisateurs de ce gestionnaire de contenu se sont plaints de la destruction de leurs sites, ce qui laisse supposer que cette faille est déjà exploitée par des personnes malveillantes.

Les développeurs de *SPIP* ont publié la version 2.1.8 qui corrige cette vulnérabilité, mais ils ont également mis à jour l'écran de sécurité en version 0.9.7 afin de prendre en compte cette faille. Le CERTA recommande le déploiement de ces correctifs.

#### Documentation

- Avis CERTA-2011-AVI-018 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-018/
- Annonce de la version 2.1.8 de SPIP du 14 janvier 2011 :
  http://www.spip-contrib.net/SPIP-2-1-8-corrige-une-importante-faille-de-securite

# 3 Imprimantes et copieurs multifonctions : pensez à la sécurité

La reprographie et l'informatique ont fini par converger. Un appareil d'impression professionnel actuel offre de multiples fonctions : impression en réseau, réimpression, envoi par courriel, gestion de comptes, de quotas, administration à distance et/ou centralisée, télémaintenance, numérisation, photocopie... Certains appreils permettent également d'émettre et de recevoir des télécopies, pourvu qu'ils soient reliés à une ligne téléphonique.

Cette richesse fonctionnelle repose sur une infrastructure matérielle qui fait de l'appareil un ordinateur à part entière. Un appareil d'impression ou de reprographie doit donc être pris en compte dans la politique de sécurité du système d'information (PSSI).

## 3.1 Exemples de risques

Les risques que font courir ces appareils perfectionnés sont de plusieurs ordres. Ils proviennent des fonctions elle-mêmes, des architectures, du cycle de vie et des matériels eux-mêmes. Ce découpage est simplifié, les causes se combinant dans bien des cas.

Quelques fonctions illustrent parfaitement l'augmentation des risques qui accompagne l'enrichissement des fonctionnalités.

La commande d'impression ou d'envoi de télécopie à partir d'un poste client est rarement authentifiée. Cette faiblesse permet une forme particulière d'injection de code indirecte, appelée parfois *cross site printing*. Cette injection est décrite dans un bulletin d'actualité du CERTA (voir section Documentation).

L'allocation de quotas ou la personnalisation du droit d'imprimer en couleur n'a de sens que si une authentification robuste est disponible.

La fonction de réimpression, activée sans garde-fou comme la création de comptes et l'utilisation de codes personnels, permet à quiconque d'imprimer le document d'autres utilisateurs. Cett fonction induit la présence sur l'appareil d'une mémoire non volatile, un disque en général, et un non-effacement des fichiers imprimés ou numérisés. Ce disque est donc une proie pour celui qui veut copier des informations.

En particulier, l'intervention sur l'appreil d'un technicien extérieur peut être l'occasion d'une copie des fichiers restants. La fin de vie de l'appareil ou du disque, gérée sans précaution, pose le même risque de divulgation.

Les possibilités d'impression en ligne sont courantes et permettent de mutualiser les appareils. Ce partage induit une communication indirecte entre les postes de travail client, donc de propagation d'infection ou de contournement de cloisonnement, si la politique d'impression n'a pas pris en considération ce cloisonnement.

Les appareils qui remplissent à la fois les fonctions d'imprimante partagée et de télécopieur disposent d'une double connexion : le réseau de données de l'administration (ou de l'entreprise) et le réseau téléphonique public. Ce dernier fait rarement l'objet de filtrage, en particulier pour les appels entrants en fonction de l'appelant. Les appareils sont des passerelles qui contournent les protections périmétriques du réseau de données.

Certains appareils permettent la télémaintenance par liaison téléphonique. Lorsque l'appareil est utilisé comme télécopieurs, il est branché en permanence sur le réseau téléphonique. L'organisme utilisateur ne peut donc contrôler les interventions du mainteneur par activation/désactivation de la liaison. La liaison est donc constamment disponible, en particulier pour des attaquants. Trop souvent, le mot de passe est faible ou est public (mot de passe usine disponible dans la documentation en ligne). Circonstance aggravante, la télémaintenance donne trop souvent des droits étendus sur l'appareil. Un attaquant qui utilise cette porte d'entrée peut sévir sans trop d'entrave.

Les liaisons non filaires avec ces appareils induisent des risques supplémentaires (Bluetooth, WiFi, etc.).

Des appareils bavards remontent au fabriquant les niveaux des consommables ou les compteurs (nombre de copies). Ces informations peuvent, dans des mains indésirables, faciliter des opérations d'intelligence économique.

Les appareils qui offrent des possibilités d'administration à distance embarquent des serveurs. Ceux-ci sont moins facilement mis à jour que des serveurs classiques, soit par conception, soit parce que ces appareils sont oubliés. Comme tous les logiciels, ces serveurs présentent des vulnérabilités, exploitables pour diverses malversations. Certaines sont exploitables pour prendre le contrôle complet du système d'impression. Des exemples sont donnés dans la section documentation.

### 3.2 Recommandations

Ce tableau peu reluisant sur le plan de la sécurité ne doit pas décourager. Le point le plus important est de considérer les appareils d'impression et de numérisation comme des ordinateurs à part entière et de les intégrer à la politique de sécurité.

Des recommandations publiques, liées à la politique d'impression ou à la sécurité pour ces appareils, sont listées dans la section documentation.

### 3.3 Documentation

- Politique d'impression des services de l'État - Guide pratique :
  http://www.industrie.gouv.fr/pratique/cimir/guidepolitimpress.pdf
- Fiche de recommandations et de bonnes pratiques relative à la sécurité des [photo]copieurs numériques du 27 novembre 2003 :
  http://www.circulaires.gouv.fr/pdf/2009/04/cir_1254.pdf
- Méthode EBIOS - Base de connaissances, version du 25 janvier 2010 :
  http://www.ssi.gouv.fr/IMG/pdf/EBIOS-2-BasesDeConnaissances-2010-01-25.pdf
- Note d'information du CERTA « Sécurité des réseaux sans fil Buetooth » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-INF-003/CERTA-2007-INF-003.html
- Note d'information du CERTA « Filtrage et pare-feux » :
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-INF-001/CERTA-2006-INF-001.html
- Bulletin d'actualité du CERTA CERTA-2008-ACT-002 (§ 3) :
  http://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-002/CERTA-2008-ACT-002.html
- Avis du CERTA - Exemples de vulnérabilités d'imprimantes et de copieurs multifonctions :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-527/
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-201/
  http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-446/

## 4 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/

# 5 Rappel des avis émis

Dans la période du 14 au 20 janvier 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-013 : Vulnérabilité dans sudo
- CERTA-2011-AVI-014 : Vulnérabilité dans BlackBerry Enterprise Server
- CERTA-2011-AVI-015 : Vulnérabilités dans HP OpenView Network Node Manager
- CERTA-2011-AVI-016 : Multiples vulnérabilités dans Google Chrome
- CERTA-2011-AVI-017 : Vulnérabilités dans SAP
- CERTA-2011-AVI-018 : Vulnérabilité dans SPIP
- CERTA-2011-AVI-019 : Vulnérabilité dans HP LoadRunner
- CERTA-2011-AVI-020 : Vulnérabilité dans IBM Websphere MQ
- CERTA-2011-AVI-021 : Vulnérabilités dans IBM WebSphere Application Server
- CERTA-2011-AVI-022 : Multiples vulnérabilités dans les produits Oracle
- CERTA-2011-AVI-023 : Vulnérabilité dans Asterisk
- CERTA-2011-AVI-024 : Vulnérabilité dans Citrix Provisionning Services
- CERTA-2011-AVI-025 : Vulnérabilités dans Cisco ASA
- CERTA-2011-AVI-026 : Vulnérabilités dans Cisco IOS

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

- CERTA-2010-AVI-420-001 : Multiples vulnérabilités dans Mozilla Firefox et Mozilla SeaMonkey (Ajout de la référence au bulletin de sécurité Oracle Solaris)
- CERTA-2010-AVI-508-001 : Multiples vulnérabilités dans les produits Mozilla (Ajout des CVE CVE-2010-3175, CVE-2010-3176 et de la référence au bulletin de sécurité Oracle Solaris)
- CERTA-2010-AVI-521-001 : Multiples vulnérabilités dans des produits Mozilla (ajout de la référence au bulletin de sécurité Oracle Solaris)

# 6 Actions suggérées

## 6.1 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.

## 6.2 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.

## 6.3 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.

## 6.4 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.

## 6.5 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.

## 6.6 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.

## 6.7 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

# 7 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.

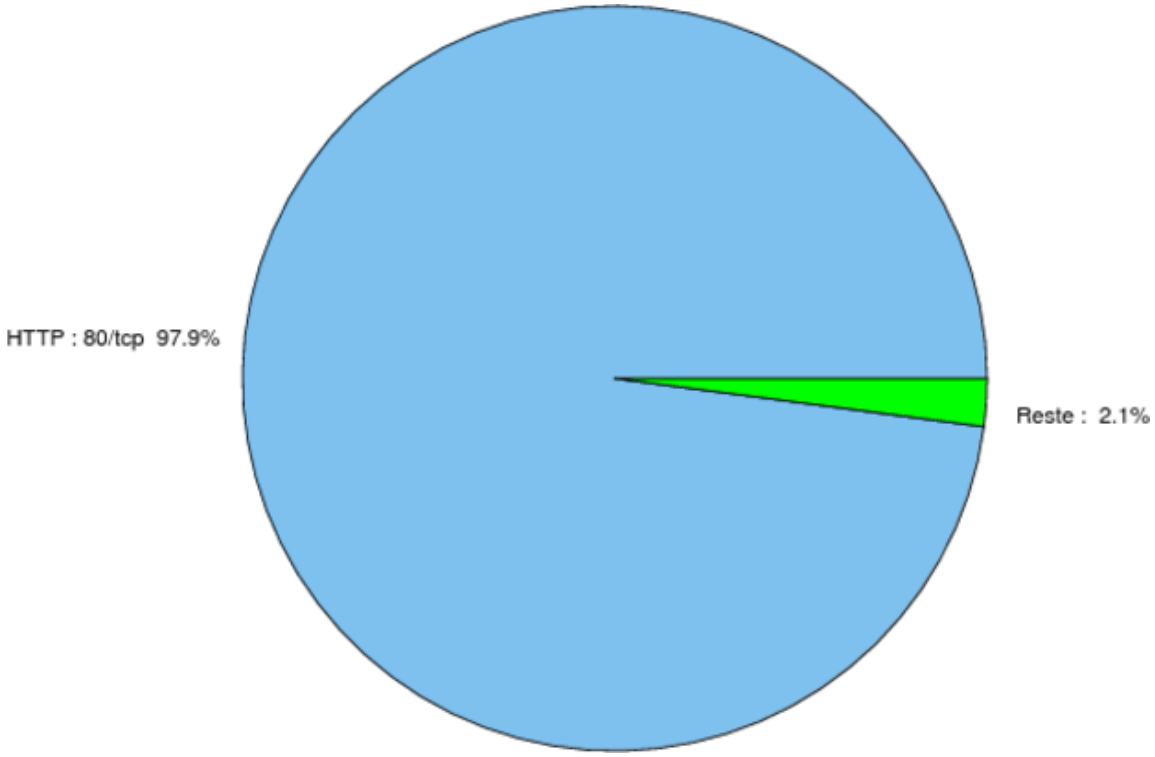


FIG. 1: Répartition relative des ports pour la semaine du 14 au 20 janvier 2011

| port | pourcentage |
|---|---|
| 80/tcp | 98.03 |
| 25/tcp | 0.76 |
| 1433/tcp | 0.3 |
| 23/tcp | 0.23 |
| 3128/tcp | 0.15 |
| 445/tcp | 0.14 |
| 22/tcp | 0.1 |
| 1080/tcp | 0.08 |
| 3389/tcp | 0.07 |
| 3306/tcp | 0.02 |
| 10080/tcp | 0.01 |

TAB. 2: Paquets rejetés

# Liste des tableaux



# Gestion détaillée du document

**21 janvier 2011** version initiale.