

Affaire suivie par :  
CERTA

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité 2011-10

---

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-010>

---

### Gestion du document

|                             |                              |
|-----------------------------|------------------------------|
| Référence                   | CERTA-2011-ACT-010           |
| Titre                       | Bulletin d'actualité 2011-10 |
| Date de la première version | 11 mars 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-010.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-010/>

## 1 Réseau privé et RFC 1918

Dans le cadre du traitement des incidents, le CERTA est parfois amené à constater que des réseaux privés ne respectent pas la RFC 1918. Ce document précise quels sont les blocs d'adresse IP qui peuvent être utilisés pour l'adressage des réseaux privés. En particulier, il s'agit :

- de la classe 10/8, qui comporte 16777216 adresses ;
- des classes 172.16/12, ce qui représente 1048576 adresses ;
- des classes 192.168/16, soit 65536 adresses.

Toutefois, de nombreux réseaux utilisent des adresses IP publiques qui, souvent, ne leur appartiennent pas. Une erreur commune est de penser que cela n'a aucune incidence. Pourtant :

- les adresses IP publiques utilisées appartenant à d'autres organismes, celles-ci sont susceptibles d'être attribuées par exemple à des serveurs. Il est probable dans ce cas que ces serveurs ne soient plus visibles (donc plus accessibles) depuis le réseau privé, pour des raisons de routage interne ;

- de la même façon, les véritables propriétaires des adresses IP publiques pourraient être bloqués par des règles de filtrage (*ingress filtering*) et se verraient ainsi dans l'impossibilité de communiquer avec certains serveurs ;
- enfin, la lecture des journaux, notamment en cas d'incident, devient particulièrement complexe, la traçabilité n'étant pas correctement assurée.

Pour ces raisons, il est fortement recommandé d'avoir recours exclusivement à un adressage conforme à la RFC 1918 pour les réseaux privés.

### Documentation

- RFC 1918 :  
<http://tools.ietf.org/html/rfc1918>

## 2 Mise à jour 4.3 du système IOS d'Apple

Apple a publié la dernière version de son OS pour iPhone 3GS et supérieur, iPod touch troisième génération et supérieur et iPad. Cette mise à jour corrige plusieurs vulnérabilités, dont certaines concernent *WebKit* et permettent l'exécution de code arbitraire à distance au moyen d'une page Web spécialement conçue.

Commercialisé depuis juillet 2008 l'iPhone 3G ne peut recevoir la version 4.3 d'iOS et aucune correction de vulnérabilités n'est disponible pour le moment. Pour rappel, l'iPhone EDGE (première génération), commercialisé un peu moins d'un an avant le 3G ne reçoit plus de mise à jour depuis la sortie de la version 3.1.3 (février 2010) et est vulnérable à un certain nombre d'attaques.

Le CERTA recommande d'effectuer la mise à jour 4.3 sur les appareils compatibles dès que possible.

### Documentation

- Bulletin de sécurité Apple HT4564 du 09 mars 2011 :  
<http://support.apple.com/kb/HT4564>
- Avi CERTA-2011-AVI-151 du 11 mars 2011 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-151/>

## 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 04 au 10 mars 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-131 : Multiples vulnérabilités dans Moodle
- CERTA-2011-AVI-132 : Vulnérabilités dans syslog-ng
- CERTA-2011-AVI-133 : Vulnérabilité dans PyWebDAV
- CERTA-2011-AVI-134 : Multiples vulnérabilités dans iTunes
- CERTA-2011-AVI-135 : Vulnérabilité dans LibTIFF
- CERTA-2011-AVI-136 : Vulnérabilité dans Apache Subversion
- CERTA-2011-AVI-137 : Vulnérabilité dans Cisco Security Agent
- CERTA-2011-AVI-138 : Vulnérabilité dans Novell Vibe OnPrem
- CERTA-2011-AVI-139 : Vulnérabilité dans EnterpriseDB Postgres Plus Advanced Server
- CERTA-2011-AVI-140 : Vulnérabilités dans Windows Media
- CERTA-2011-AVI-141 : Vulnérabilité dans Microsoft Groove
- CERTA-2011-AVI-142 : Vulnérabilité dans le client Remote Desktop de Windows
- CERTA-2011-AVI-143 : Multiples vulnérabilités dans VMware ESX/ESXi
- CERTA-2011-AVI-144 : Multiples vulnérabilités dans Joomla!
- CERTA-2011-AVI-145 : Vulnérabilité dans Ubuntu
- CERTA-2011-AVI-146 : Vulnérabilité dans Postfix
- CERTA-2011-AVI-147 : Vulnérabilité dans Apache Archiva
- CERTA-2011-AVI-148 : Vulnérabilités dans Google Chrome

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

- CERTA-2010-AVI-555-002 : Vulnérabilité dans OpenSSL (Ajout de la référence au bulletin de sécurité HP-UX)
- CERTA-2010-AVI-590-001 : Vulnérabilités dans OpenSSL (Ajout de la référence au bulletin de sécurité HP-UX)
- CERTA-2011-AVI-093-001 : Multiples vulnérabilités dans Oracle Java (ajout de la mise à jour de Java pour les systèmes Mac OS X)

## 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](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.

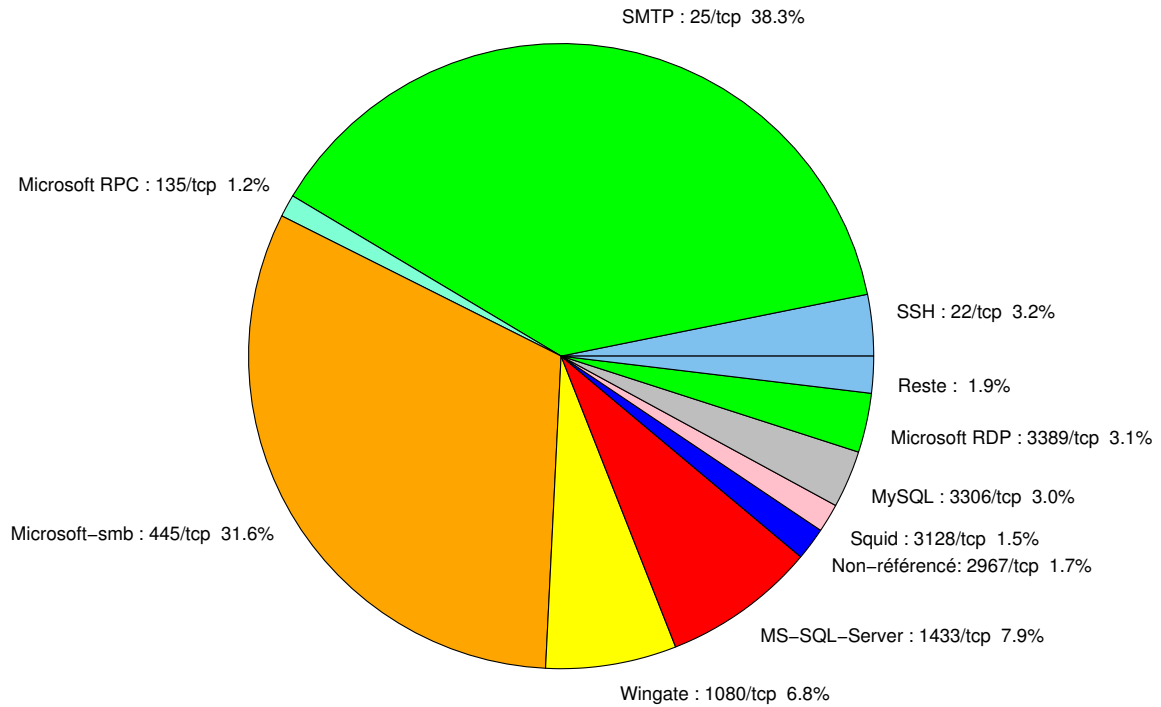


FIG. 1: Répartition relative des ports pour la semaine du 04 au 10 mars 2011

| port     | pourcentage |
|----------|-------------|
| 25/tcp   | 38.26       |
| 445/tcp  | 31.6        |
| 1433/tcp | 7.92        |
| 1080/tcp | 6.76        |
| 80/tcp   | 4.75        |
| 22/tcp   | 3.17        |
| 3389/tcp | 3.06        |
| 3306/tcp | 2.95        |
| 2967/tcp | 1.69        |
| 3128/tcp | 1.47        |
| 135/tcp  | 1.16        |
| 23/tcp   | 0.63        |
| 4899/tcp | 0.42        |
| 3127/tcp | 0.1         |

TAB. 2: Paquets rejetés

## Liste des tableaux

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

## Gestion détaillée du document

11 mars 2011 version initiale.