



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 juin 2011
N° CERTA-2011-ACT-024

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-24

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-024>

Gestion du document

Référence	CERTA-2011-ACT-024
Titre	Bulletin d'actualité 2011-24
Date de la première version	17 juin 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.

1 Outil de détection de vulnérabilités pour WordPress

Un outil de détection de vulnérabilités, spécifiquement conçu pour *WordPress*, a récemment été publié sur l'Internet. Ses fonctionnalités permettent notamment d'obtenir une liste de comptes utilisateur, de vérifier la présence de mots de passe faibles et d'afficher les vulnérabilités connues en fonction de la version de *WordPress* installée. Il est prévu, pour de futures versions de ce scanner, d'ajouter la prise en compte des différents modules.

S'il est évident qu'un tel outil présente un intérêt pour un administrateur de sites Web ou pour un RSSI, il en est de même pour un attaquant. Il faut donc s'attendre à ce que ce scanner, sous licence GPLv3, soit utilisé à des fins malveillantes, soit modifié afin d'exploiter automatiquement des vulnérabilités détectées.

Il ne serait pas surprenant que d'autres outils, conçus pour traiter d'autres gestionnaires de contenu, soient prochainement créés, afin de prendre en compte les spécificités et vulnérabilités liées aux modules de chacun.

Le CERTA rappelle, qu'outre l'installation des correctifs de sécurité, il est envisageable de déployer un serveur mandataire inverser (*reverse proxy*), de mettre en place du filtrage ou encore de limiter l'utilisation des modules (pour les gestionnaires de contenu).

2 Mise à jour Microsoft du mois de juin

Microsoft a publié cette semaine un nombre élevé de mises à jour pour ses différents logiciels. On dénombre en effet 17 bulletins émis pour un total de 32 vulnérabilités corrigées.

Parmi ces bulletins, dix traitent de vulnérabilités permettant une exécution de code arbitraire à distance et 9 sont classés comme étant critiques par l'éditeur.

Microsoft a publié, dans ces bulletins, des mises à jour corrigeant des vulnérabilités affectant Internet Explorer 6, 7, 8 et 9 qui sont d'ores et déjà activement exploitées.

Documentation

- Résumé du bulletin de sécurité Microsoft de juin 2011 :
<https://www.microsoft.com/technet/security/bulletin/ms11-jun.msp>

3 Publication de nouvelles mises à jour d'Adobe

Cette semaine, Adobe a publié cinq bulletins de sécurité (apsb11-14 à apsb11-18) concernant les produits :

- Adobe Reader et Acrobat ;
- Adobe Flash Player ;
- Adobe Shockwave Player ;
- Adobe Cold Fusion ;
- Adobe LifeCycle Data Services et BlazeDS.

Les vulnérabilités concernant Adobe Reader et Acrobat, Adobe Flash Player et Adobe Shockwave Player permettent l'exécution de code arbitraire à distance pour les systèmes Windows, Mac et Linux. Il est impératif d'appliquer les mises à jour dès que possible.

Documentation

- Avis de sécurité du CERTA CERTA-2011-AVI-340 du 15 juin 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-340/index.html>
- Avis de sécurité du CERTA CERTA-2011-AVI-341 du 15 juin 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-341/index.html>
- Avis de sécurité du CERTA CERTA-2011-AVI-342 du 15 juin 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-342/index.html>
- Avis de sécurité du CERTA CERTA-2011-AVI-343 du 15 juin 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-343/index.html>
- Avis de sécurité du CERTA CERTA-2011-AVI-344 du 15 juin 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-344/index.html>

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 10 au 16 juin 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-337 : Vulnérabilité dans HP OpenView Data Storage Protector
- CERTA-2011-AVI-338 : Vulnérabilité dans Horde
- CERTA-2011-AVI-339 : Vulnérabilité dans Ruby on Rails
- CERTA-2011-AVI-340 : Multiples vulnérabilités dans Adobe ColdFusion
- CERTA-2011-AVI-341 : Multiples vulnérabilités dans Adobe LifeCycle Data Services, LifeCycle ES et BlazeDS
- CERTA-2011-AVI-342 : Multiples vulnérabilités dans Adobe Reader et Acrobat
- CERTA-2011-AVI-343 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2011-AVI-344 : Vulnérabilité dans Adobe Flash Player
- CERTA-2011-AVI-345 : Vulnérabilité dans Microsoft Windows MHTML
- CERTA-2011-AVI-346 : Vulnérabilité dans Microsoft OLE Automation
- CERTA-2011-AVI-347 : Vulnérabilité dans NET Framework et Microsoft Silverlight
- CERTA-2011-AVI-348 : Vulnérabilité dans Threat Management Gateway
- CERTA-2011-AVI-349 : Vulnérabilité dans les pilotes en mode noyau du système Microsoft Windows
- CERTA-2011-AVI-350 : Vulnérabilités dans le système de fichiers distribués (DFS) de Microsoft
- CERTA-2011-AVI-351 : Vulnérabilité dans le client SMB de Microsoft
- CERTA-2011-AVI-352 : Vulnérabilité dans Microsoft NET Framework
- CERTA-2011-AVI-353 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2011-AVI-354 : Vulnérabilité dans le composant AFD de Microsoft
- CERTA-2011-AVI-355 : Vulnérabilité dans Hyper-V
- CERTA-2011-AVI-356 : Vulnérabilité dans le serveur SMB de Microsoft Windows
- CERTA-2011-AVI-357 : Vulnérabilité de l’éditeur XML de Microsoft
- CERTA-2011-AVI-358 : Vulnérabilités dans Microsoft Internet Explorer
- CERTA-2011-AVI-359 : Vulnérabilité dans les services de certificats Active Directory de Microsoft Windows
- CERTA-2011-AVI-360 : Vulnérabilité dans le Vector Markup Language de Microsoft
- CERTA-2011-AVI-361 : Vulnérabilité dans Google Chrome

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 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.

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 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.

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.

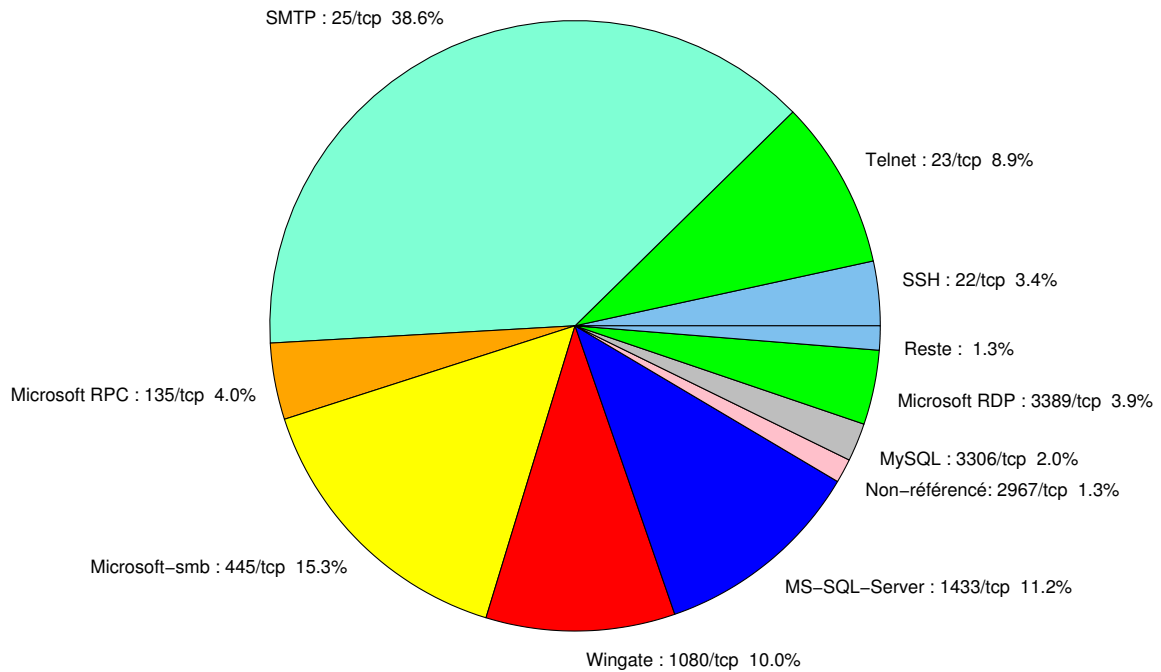


FIG. 1: Répartition relative des ports pour la semaine du 10 au 16 juin 2011

port	pourcentage
25/tcp	38.55
445/tcp	15.33
1433/tcp	11.18
1080/tcp	10.01
23/tcp	9.05
135/tcp	4.04
3389/tcp	3.94
22/tcp	3.4
80/tcp	2.34
3306/tcp	2.02
2967/tcp	1.27
3128/tcp	0.95
4899/tcp	0.21
21/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

17 juin 2011 version initiale.