Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 avril 2011
N° CERTA-2011-ACT-015

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-15

Gestion du document

Référence	CERTA-2011-ACT-015
Titre	Bulletin d'actualité 2011-15
Date de la première version	15 avril 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-015.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-015/

1 Alerte dans les produits Adobe

En début de semaine, le CERTA a émis une alerte concernant les produits Adobe. Une vulnérabilité non corrigée est en effet présente dans les produits Adobe Flash Player, Adobe Acrobat et Adobe Reader. L'alerte CERTA-2011-ALE-003 donne la liste des versions vulnérables. Un document spécialement conçu par une personne malintentionn'ee peut provoquer l'exécution de code arbitraire sur le système de la victime.

Cette vulnérabilité est actuellement activement exploitée sur l'Internet, via des documents Flash (.swf) inclus dans des fichiers au format Microsoft Word (.doc) ou Microsoft Excel (.xls) et diffusés par courrier électronique, la cible principale étant les systèmes Windows.

Adobe a annoncé la mise à disposition de mises à jour pour Adobe Flash le 15 avril 2011, jour de la publication de cet article. Toutefois, au moment de la rédaction de celui-ci, ces mises à jour ne sont pas disponibles.

Adobe indique que les mises à jour des autres produits concernés seront disponibles avant la semaine du 25 avril 2011. L'alerte sera alors modifiée au regard de ces nouvelles informations. Seule la version d'Adobe Reader X pour Windows est retardée au 14 juin 2011. Adobe considère que le *Protected Mode* empêche l'exploitation de la faille sur ce logiciel.

Il est à noter que les utilisateurs de Google Chrome peuvent déjà mettre à jour leur logiciel pour atteindre la version 10.0.648.205 corrigeant la vulnérabilité (se reporter à l'avis CERTA-2011-AVI-227).

Dans tous les cas, il reste impératif de mettre à jour les logiciels déclarés vulnérables dès la sortie des correctifs.

Documentation

- Alerte CERTA-2011-ALE-003 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-003/index.html
- Avis CERTA-2011-AVI-227 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-227/index.html

2 Mise à jour Microsoft du mois d'avril

Cette semaine, *Microsoft* a publié un nombre élevé de mises à jour pour ses différents logiciels. En effet, ce ne sont pas moins de 17 bulletins qui ont été émis pour un total de 64 vulnérabilités corrigées. Parmi ces bulletins, 16 traitent de vulnérabilités autorisant une exécution de code arbitraire à distance et 9 sont classés comme étant critiques par l'éditeur.

Deux de ces vulnérabilités retiennent particulièrement l'attention. Il s'agit de deux failles critiques autorisant l'exécution de code arbitraire à distance, exposées dans les bulletins MS11-019 et MS11-020, et qui concernent respectivement le client et le serveur *SMB* de *Microsoft Windows*. De part leur complémentarité, ces deux vulnérabilités sont particulièrement dangereuses. En effet, un ver utilisant ces vulnérabilités comme mécanisme de propagation pourrait aisément compromettre l'ensemble d'un réseau suite à la contamination d'un serveur ou d'un simple poste client. Il est donc impératif de mettre à jour rapidement l'ensemble des systèmes *Microsoft Windows*.

Notons aussi que *Microsoft* a publié, dans ces bulletins, des mises à jour concernant des failles dans *Internet Explorer 6, 7* et *8* ainsi que dans le protocole *MHMTL* qui sont d'ores et déjà activement exploitées. Ici encore, une mise à jour dans les plus brefs délais s'impose.

D'autres parts, des mises à jour *Microsoft Office, Excel* et *Powerpoint* sont aussi présentes. Bien que classées comme importantes et non comme critiques par l'éditeur, il convient d'appliquer les mises à jour et de rappeler aux utilisateurs d'être vigilant à l'égard des pièces jointes.

Par ailleurs, il semblerait que la mise à jour MS11-025 concernant la bibliothèque *Microsoft Foundation Class* pose problème avec certains logiciels. Cependant, aucune note officielle de *Microsoft* ou des éditeurs concernés ne confirme cet état de fait.

Documentation

- Résumé du bulletin de sécurité Microsoft d'avril 2011 :
  https://www.microsoft.com/technet/security/bulletin/ms11-apr.mspx

3 User Shell Folders et problèmes applicatifs

Il existe au sein de la base de registre de Microsoft Windows des clés de registre nommées *Shell Folders* et *User Shell Folders* permettant de stocker les chemins d'accès de différents répertoires jouant un rôle particulier pour le système d'exploitation. Ces clés se situent respectivement aux emplacements suivants :

```
HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders

HKEY_CURRENT_USER\software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
```

Des valeurs enregistrent, par exemple, le chemin d'accès au répertoire « Mes Documents », au bureau ou à l'endroit où sont stockés les fichiers de session. Dans les dernières versions du système d'exploitation de Microsoft, les répertoires des bibliothèques d'images, de musiques ou de vidéos sont également référencés.

Si l'une de ces valeurs pointe sur un lecteur et que ce dernier est inaccessible lors de l'installation ou de la suppression d'une application, Microsoft Windows affiche alors une erreur et stoppe le processus en cours d'exécution. Ce type d'erreur peut donc facilement bloquer le déploiement d'une application ou d'une mise à jour.

Le problème est connu chez Microsoft qui a publié un « *Fix it* » (cf. la section Documentation). Ce problème est également connu chez Adobe qui a publié un article dans sa base de connaissance (cf. la section Documentation). Le CERTA recommande donc d'utiliser avec précaution le changement de ces valeurs afin d'éviter tout problème lors du déploiement de nouvelles applications ou de mises à jour.

Documentation

- Article #886549 de la base de connaissance de Microsoft :
  http://support.microsoft.com/kb/886549
- Article #404946 de la base de connaissance d'Abobe :
  http://kb2.adobe.com/cps/404/kb404946.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 8 au 14 avril 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-ALE-003 : Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat
- CERTA-2011-AVI-197 : Vulnérabilité dans IBM Virtual I/O Server
- CERTA-2011-AVI-198 : Vulnérabilités dans RoundCube
- CERTA-2011-AVI-199 : Vulnérabilité dans McAfee Firewall Reporter
- CERTA-2011-AVI-200 : Vulnérabilité dans Novell ZENworks Configuration Management
- CERTA-2011-AVI-201 : Vulnérabilités dans Internet Explorer
- CERTA-2011-AVI-202 : Vulnérabilités dans le client SMB de Microsoft
- CERTA-2011-AVI-203 : Vulnérabilité dans le serveur SMB de Microsoft Windows
- CERTA-2011-AVI-204 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2011-AVI-205 : Vulnérabilités dans Microsoft PowerPoint

- CERTA-2011-AVI-206 : Vulnérabilités dans Microsoft Office
- CERTA-2011-AVI-207 : Vulnérabilité dans Fax Cover Page Editor de Microsoft
- CERTA-2011-AVI-208 : Vulnérabilité dans la bibliothèque MFC
- CERTA-2011-AVI-209 : Vulnérabilité dans le gestionnaire de protocole MHTML de Microsoft Windows
- CERTA-2011-AVI-210 : Multiples vulnérabilités dans des contrôles ActiveX de Microsoft Windows
- CERTA-2011-AVI-211 : Vulnérabilité dans Microsoft NET Framework
- CERTA-2011-AVI-212 : Vulnérabilité dans Microsoft Windows GDI+
- CERTA-2011-AVI-213 : Vulnérabilité dans le client DNS de Microsoft Windows
- CERTA-2011-AVI-214 : Vulnérabilité dans le moteur JScript et VBScript de Microsoft Windows
- CERTA-2011-AVI-215 : Vulnérabilité dans le pilote Compact Font Format (CFF) OpenType
- CERTA-2011-AVI-216 : Vulnérabilité dans le convertisseur de texte de WordPad
- CERTA-2011-AVI-217 : Multiples vulnérabilités dans des pilotes en mode noyau du système Microsoft Windows
- CERTA-2011-AVI-218 : Vulnérabilité dans VLC
- CERTA-2011-AVI-219 : Vulnérabilités dans HP Network Node Manager i
- CERTA-2011-AVI-220 : Vulnérabilités dans OTRS
- CERTA-2011-AVI-221 : Multiples vulnérabilités dans BlackBerry Enterprise Server
- CERTA-2011-AVI-222 : Vulnérabilité dans MIT Kerberos
- CERTA-2011-AVI-223 : Multiples vulnérabilités dans BlackBerry Enterprise Server

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2011-AVI-190-001 : Vulnérabilité dans le client DHCP ISC (ajout des bulletins de sécurité Red Hat et Novell)

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.

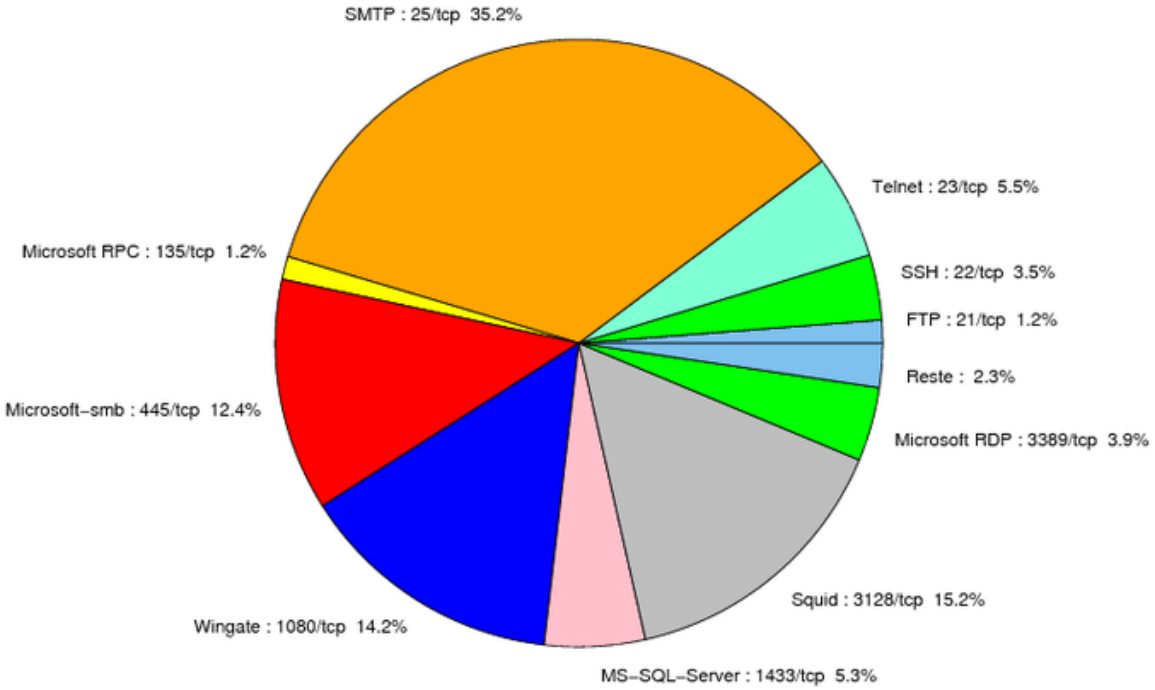

FIG. 1: Répartition relative des ports pour la semaine du 8 au 14 avril 2011

port	pourcentage
25/tcp	35.17
3128/tcp	15.19
1080/tcp	14.16
445/tcp	12.47
80/tcp	5.9
23/tcp	5.62
1433/tcp	5.34
3389/tcp	3.93
22/tcp	3.47
135/tcp	1.21
3306/tcp	0.93
2967/tcp	0.46
4899/tcp	0.18
10080/tcp	0.09

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

15 avril 2011 version initiale.