Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 avril 2011
N° CERTA-2011-ACT-016

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-16

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-016`

Gestion du document

Référence	CERTA-2011-ACT-016
Titre	Bulletin d'actualité 2011-16
Date de la première version	22 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-016.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-016/

1 Le format de texte enrichi véhicule de logiciels malveillants

Le CERTA traite de plus en plus régulièrement des incidents dans lesquels l'origine de la compromission est un document RTF spécialement conçu pour exploiter des vulnérabilités dans les logiciels permettant d'afficher ce format.

Le Rich Text Format, ou format de texte enrichi, est un format de fichier créé par Microsoft, et supporté par de nombreux logiciels de traitement de texte. Il permet de créer des documents aux textes formattés.

À l'instar des formats PDF ou DOC, les documents RTF peuvent également être vecteurs de contenus malveillants tentant d'exploiter des vulnérabilités de traitements de texte. Une des cibles privilégiées par les attaquants est Microsoft Word, via la vulnérabilité identifiée par le numéro CVE CVE-2010-3333 et détaillée dans l'avis CERTA-2010-AVI-543. Particulièrement intéressante pour un attaquant, cette vulnérabilité permet l'exécution de code arbitraire à distance, est aisément exploitable, et existe sur de nombreuses versions du logiciel Microsoft Word pour les systèmes Windows comme MacOS. En outre, le format RTF est souvent, à tort, considéré comme inoffensif et l'utilisateur est plus susceptible d'ouvrir ce type de fichier.

D'autres vulnérabilités exploitables au travers de documents RTF ont été identifiées par le passé dans d'autres produits. On pourra citer par exemple les vulnérabilités CVE-2010-3451 et CVE-2010-3452 affectant des versions d'OpenOffice.org.

L'attention récente apportée aux documents PDF reçus en pièces jointes de courriers électroniques ne doit pas réduire la vigilance apportée à l'ensemble des documents échangés par ce biais. Aucun format de fichier ne doit être considéré comme inoffensif. Les différents formats sont régulièrement sujets à modifications, comme l'ajout de nouvelles fonctionalités, et les nombreux logiciels permettant de les afficher sont autant de vecteurs de compromission éventuels que ciblent les attaquants.

Documentation

- Avis CERTA-2010-AVI-543, traitant de la vulnérabilité CVE-2010-3333 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-543/
- Avis CERTA-2010-AVI-372, traitant des vulnérabilités CVE-2010-3451 et CVE-2010-3452 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-372/
- Avis CERTA-2010-AVI-039, traitant des vulnérabilités CVE-2010-1901 et CVE-2010-1902 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-039/

2 Osboléscence de Ubuntu 9.10

Comme cela était planifié dans le cycle de vie de cette distribution `GNU/Linux`, la version 9.10 de `Ubuntu` arrivera en fin de support le 30 avril 2011. Le responsable de sortie de version en a d'ailleurs fait l'annonce fin mars 2011 : `https://lists.ubuntu.com/archives/ubuntu-announce/2011-March/000142.html`.

La politique de cycle de vie chez `Ubuntu` est en effet très claire : les versions « normales » sont supportées deux ans alors que les versions estampillées *LTS* (pour *Long Term Support*) sont maintenues pendant cinq ans. Ainsi la version 6.06 est encore mise à jour à la date de ce bulletin et jusqu'au 30 juin 2011.

Bien que 2 ans soit déjà une durée confortable permettant la planification d'une mise à jour de version, il est tout de même recommandé d'utiliser des versions *LTS* pour des projets à long terme ou relativement complexes à mettre en œuvre.

Concernant la version 9.10, il est vivement recommandé à ses utilisateurs de migrer vers une version plus récente encore supportée.

3 Protection en profondeur et vulnérabilités

Lors de la conférence *Infiltrate* qui s'est tenue les 16 et 17 avril 2011 en Floride, les experts en sécurité Chris Valasek et Ryan Smith ont démontré qu'il était possible de contourner certaines protections anti-exploitation mises en place par *Microsoft* dans son système *Windows*. Leur attaque se base sur une vulnérabilité (CVE-2011-3972), aujourd'hui corrigée, de type dépassement de tampon (*heap-overflow*) présente dans *IIS* 7.

Malgré la présence des mécanismes de protection étendus mis en place par *Microsoft* afin de prévenir l'exécution de code, ces deux chercheurs ont réussi à prendre le contrôle de la machine vulnérable.

Cette attaque présente en soi un caractère relativement nouveau, puisque les protections mises en place au niveau du tas se sont révélées robustes. En fait, plutôt que de s'attaquer directement au système de protection et de tenter de le contourner, les deux chercheurs ont tout simplement réussi à le désactiver. Ils ont en fait forcé le programme à modifier sa gestion du tas pour qu'il utilise le mode *Low-Fragmentation Heap* introduit avec *Windows Vista*. Ce mode de gestion permet au programme de minimiser la fragmentation du tas et d'optimiser ainsi l'espace. Mais en contrepartie, toutes les protections du tas sont désactivées. A partir de cet instant, il devient relativement aisé d'exploiter la faille avec des techniques classiques.

Cet exemple démontre qu'aucun mécanisme de protection n'est infaillible, aussi sophistiqué soit-il. Il convient donc de s'appuyer sur une défense en profondeur qui multipliera les difficultés imposées à l'attaquant.

Documentation

- Windows function disable exploit protection: http://www.h-online.com/security/news/item/Windows-function-disables-exploit-protection-1229943.html

- Preventing the exploitation of user mode heap corruption vulnerabilities : http://blogs.technet.com/b/srd/archive/2009/08/04/preventing-the-exploitation-of-user-mode-heap-corruption-vulnerabilities.aspx
- MSDN Low-fragmentation Heap : http://msdn.microsoft.com/en-us/library/aa366750(v=vs.85).aspx
- CVE Référence CVE-2010-3972 : http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3972

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 15 au 21 avril 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-225 : Vulnérabilité dans Dotclear
- CERTA-2011-AVI-226 : Vulnérabilités dans Safari
- CERTA-2011-AVI-227 : Vulnérabilités dans Google Chrome
- CERTA-2011-AVI-228 : Vulnérabilités dans Apple iOS
- CERTA-2011-AVI-229 : Vulnérabilités dans CA Total Defense
- CERTA-2011-AVI-230 : Multiples vulnérabilités dans Joomla!
- CERTA-2011-AVI-231 : Vulnérabilités dans kde4libs
- CERTA-2011-AVI-232 : Vulnérabilités dans Wireshark
- CERTA-2011-AVI-233 : Vulnérabilités dans SAP NetWeaver Web Application Server
- CERTA-2011-AVI-234 : Vulnérabilité de Adobe Flash Player
- CERTA-2011-AVI-235 : Multiples vulnérabilités dans itunes
- CERTA-2011-AVI-236 : Vulnérabilité dans RSA Adaptive Authentication
- CERTA-2011-AVI-237 : Vulnérabilité dans HP Network Node Manager i
- CERTA-2011-AVI-238 : Multiples Vulnérabilités dans les produits Oracle

– CERTA-2011-AVI-239 : Multiples Vulnérabilités dans les produits Oracle Sun
– CERTA-2011-AVI-240 : Multiples Vulnérabilités dans HP Systems Management Homepage
– CERTA-2011-AVI-241 : Multiples Vulnérabilités dans HP Systems Insight Manager
– CERTA-2011-AVI-242 : Multiples vulnérabilités dans HP Insight Control
– CERTA-2011-AVI-243 : Vulnérabilités dans IBM Lotus Symphony
– CERTA-2011-AVI-244 : Vulnérabilité dans HP Virtual Server Environment pour Windows
– CERTA-2011-AVI-245 : Vulnérabilité dans les systèmes FreeBSD
– CERTA-2011-AVI-246 : Vulnérabilité dans HP Performance Insight

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

– CERTA-2011-ALE-003-003 : Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat (annonce des dates de publication des correctifs)
– CERTA-2011-AVI-218 : Vulnérabilité dans VLC (ajout du numéro de CVE)
– CERTA-2011-AVI-224-001 : Vulnérabilité dans IBM Tivoli Directory Server (ajout du numéro CVE)

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.

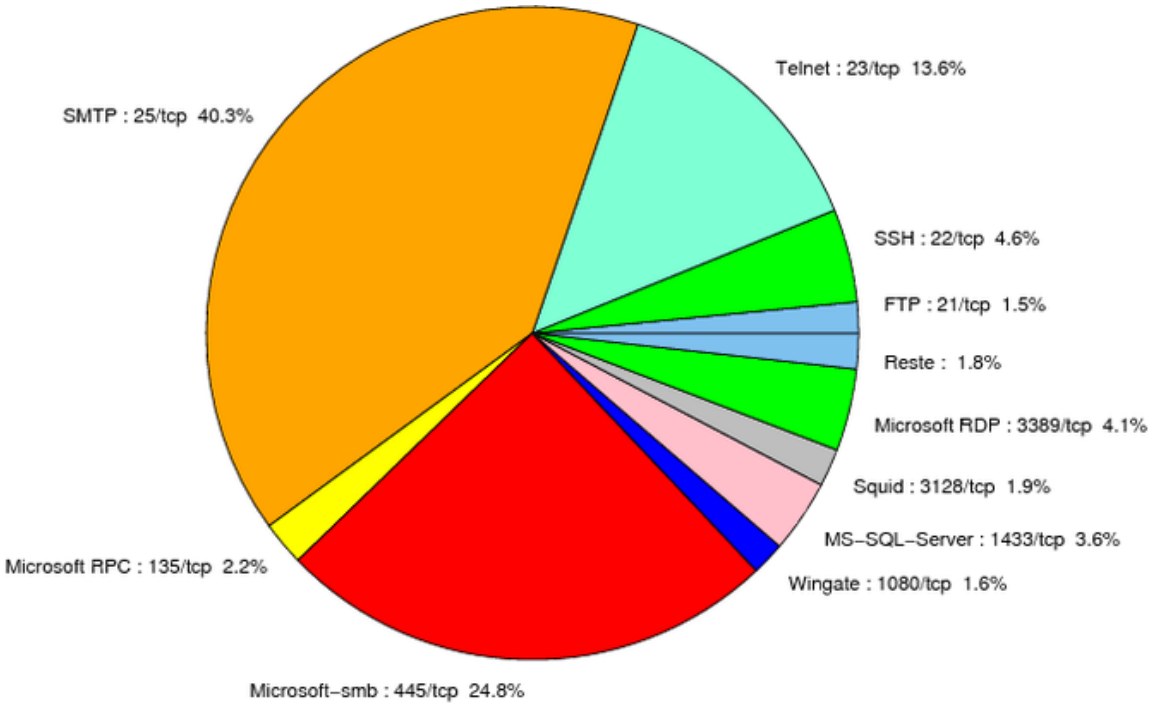

FIG. 1: Répartition relative des ports pour la semaine du 15 au 21 avril 2011

port	pourcentage
25/tcp	40.28
445/tcp	24.8
23/tcp	13.61
80/tcp	4.61
3389/tcp	4.06
1433/tcp	3.62
135/tcp	2.19
3128/tcp	1.86
1080/tcp	1.64
21/tcp	1.53
3306/tcp	0.54
4899/tcp	0.43
2967/tcp	0.21
10080/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

22 avril 2011 version initiale.