

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-29

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-029>

Gestion du document

Référence	CERTA-2011-ACT-029
Titre	Bulletin d'actualité 2011-29
Date de la première version	22 juillet 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-029.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-029/>

1 Incidents de la semaine

Fausses notifications de livraison

Les courriels prétendant avertir de la livraison de colis par coursiers sont devenus courants. Bien sûr, les délinquants de l'Internet ont sauté sur l'occasion pour transmettre de fausses notifications avec généralement des pièces jointes piégées, les liens vers les sites malveillants étant assez rares. La machine de l'imprudent qui aura ouvert la pièce jointe sera infectée par un cheval de Troie, un faux antivirus ou tout autre programme malveillant. Ces courriels frauduleux usurpent régulièrement les marques DHL, FedEx, UPS... Ils sont souvent rédigés en anglais.

Comme pour le filoutage qui a commencé par les faux sites bancaires et qui, maintenant, se diversifie (jeux en ligne, administration, fournisseurs d'énergie...), les fausses notifications couvrent un périmètre plus large.

Le CERTA a été informé de l'utilisation d'une marque française de la grande distribution qui propose un service de commande en ligne avec livraison à domicile pour expédier de fausses notifications de livraison, bien entendu avec une pièce jointe piégée. Toute marque de vente par correspondance est utilisable par les cyberdélinquants.

Dans le cas signalé, l'adresse d'expédition qui, rappelons-le, est aisément falsifiable, est crédible. Le corps de message est en français très correct. La pièce jointe est la prétendue facture, mais en fait un programme malveillant.

Recommandations

Face à ce type d'attaque, en constante évolution, la vigilance de l'utilisateur est la meilleure arme.

Lorsque l'on est client de ces services de commande et de livraison à domicile, il est pertinent d'utiliser une adresse de messagerie dédiée. Ainsi, toute notification arrivant sur une autre adresse, notamment professionnelle, sera clairement une tentative d'infection. Pour toute notification arrivant sur une adresse dédiée à cela soulevant le moindre doute, il est préférable de demander une confirmation à la marque émettrice par un canal connu antérieurement.

Les antivirus atteignent leurs limites quand les pièces jointes à l'effet identique peuvent revêtir d'innombrables apparences, parfois par des variations simples mais au spectre quasi infini de leur codage (binaire, compressions, packing, base 64, UUencodage, création du code par un script...). Comme tout outil de sécurité, les antivirus doivent être vus comme des éléments d'une architecture de défense en profondeur et non comme *La* protection.

Au niveau de l'administration ou de l'entreprise, il faut bien entendu appliquer les règles de base pour limiter la surface d'attaque et réduire les impacts :

- éduquer les utilisateurs et les faire adhérer à la politique de sécurité ;
- mettre à jour les systèmes, les logiciels, les greffons ;
- concevoir une architecture robuste pour le système d'information, intégrant la défense en profondeur ;
- durcir les configurations, notamment en supprimant les services et les applications inutiles ;
- accorder les droits minimaux aux utilisateurs ;
- superviser le fonctionnement du SI et détecter les anomalies ;
- mettre en place une procédure de réaction en cas d'incident et la faire connaître des utilisateurs ;
- réviser régulièrement les mesures, en fonction des retours et des audits.

2 Correction de l'alerte CERTA-2011-ALE-004 : Apple iOS

Apple a corrigé cette semaine les vulnérabilités (voir l'alerte *CERTA-2011-ALE-004*) impactant Apple iOS pour iPhone 4, iPhone 3GS, iPod touch 3G (et versions supérieures) et iPad.

Des codes exploitant ces vulnérabilités (notamment pour effectuer le *Jailbreak* de ces appareils) étant disponibles sur l'Internet, le CERTA recommande vivement l'installation de ces mises à jour.

Documentation

- Alerte CERTA-2011-ALE-004 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-004/index.html>
- Avis CERTA-2011-AVI-395 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-395/index.html>

3 Bibliothèques et vulnérabilités

Cette semaine, l'US-CERT a émis un avis de sécurité concernant une vulnérabilité dans la bibliothèque de conversion de fichiers `vsgdsf.dll` (`libvs_gsd.f.so` sous Linux). Il s'agit en fait d'une erreur dans l'analyseur de fichiers *CoreIDRAW* conduisant à un dépassement de tampon dans la pile.

Cette vulnérabilité, bien que classique, a un impact large, la bibliothèque fautive étant très répandue. Ainsi la faille touche un grand nombre de produits d'éditeurs différents (*Microsoft, Dell, IBM, etc...*). Cet état de fait démontre, bien entendu, la nécessité d'appliquer au plus vite la mise à jour corrigeant la vulnérabilité, mais aussi l'importance des mises à jour liées aux bibliothèques en général.

En effet, même si de prime abord une application ne semble pas touchée par une vulnérabilité, il suffit qu'elle utilise une bibliothèque vulnérable pour être à son tour exposée. En conséquence, le CERTA recommande d'accorder une attention particulière aux mises à jour concernant des bibliothèques, en vérifiant notamment leur utilisation par les applications installées.

Documentation

- Bulletin de sécurité de l'US-CERT VU#103425 du 19 juillet 2011 :
<http://www.kb.cert.org/vuls/id/103425>

4 Google alerte certains utilisateurs infectés

Cette semaine, Google a publié un article sur son *blog* afin de prévenir ses utilisateurs de la modification de la page d'accueil de son moteur de recherche en cas de détection d'un code malveillant particulier.

En effet, Google a détecté qu'une famille de codes malveillants avait pour comportement de faire passer tout le trafic Internet des machines compromises par un nombre limité de serveurs mandataires. Lorsque le moteur de recherche constate une requête en provenance de cette liste d'adresses IP, l'utilisateur est averti de la potentielle compromission de sa machine par un large bandeau jaune au dessus du champ de saisie.

Le CERTA rappelle qu'en cas de compromission d'une machine, il est conseillé de réinstaller complètement le système d'exploitation ainsi que l'ensemble des applicatifs dans leurs versions à jour des correctifs de sécurité. Selon Google, l'origine de l'infection semble être un faux antivirus. Il est recommandé de n'installer que des solutions antivirales téléchargées sur le site d'un éditeur de confiance.

5 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/>

6 Rappel des avis émis

Dans la période du 15 au 21 juillet 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-392 : Vulnérabilité dans BlackBerry Enterprise Server
- CERTA-2011-AVI-393 : Mise à jour du noyau Red Hat
- CERTA-2011-AVI-394 : Vulnérabilités dans VLC
- CERTA-2011-AVI-395 : Vulnérabilités dans Apple iOS
- CERTA-2011-AVI-396 : Vulnérabilités dans Citrix Access Gateway Plug-in

- CERTA-2011-AVI-397 : Vulnérabilités dans Wireshark
- CERTA-2011-AVI-398 : Vulnérabilité dans ArcSight Connector Appliance
- CERTA-2011-AVI-399 : Vulnérabilité de Check Point Multi-Domain Management / Provider-1
- CERTA-2011-AVI-400 : Multiples vulnérabilités dans les produits Oracle
- CERTA-2011-AVI-401 : Vulnérabilité dans JBoss
- CERTA-2011-AVI-402 : Vulnérabilité dans IBM WebSphere
- CERTA-2011-AVI-403 : Multiples vulnérabilités dans Safari
- CERTA-2011-AVI-404 : Vulnérabilités dans les produits Cisco SA 500 Series Security Appliances
- CERTA-2011-AVI-405 : Vulnérabilité dans Joomla!
- CERTA-2011-AVI-406 : Vulnérabilité dans Cisco ASR 9000 Series Routers
- CERTA-2011-AVI-407 : Vulnérabilité dans CA Gateway Security and Total Defense
- CERTA-2011-AVI-408 : Vulnérabilité dans Google Picasa

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

- CERTA-2011-ALE-004-001 : Vulnérabilités dans Apple iOS (ajout des références aux bulletins Apple et aux CVE)
- CERTA-2011-AVI-336-001 : Multiples vulnérabilités dans Java (ajout du bulletin IBM)

7 Actions suggérées

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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

8 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.

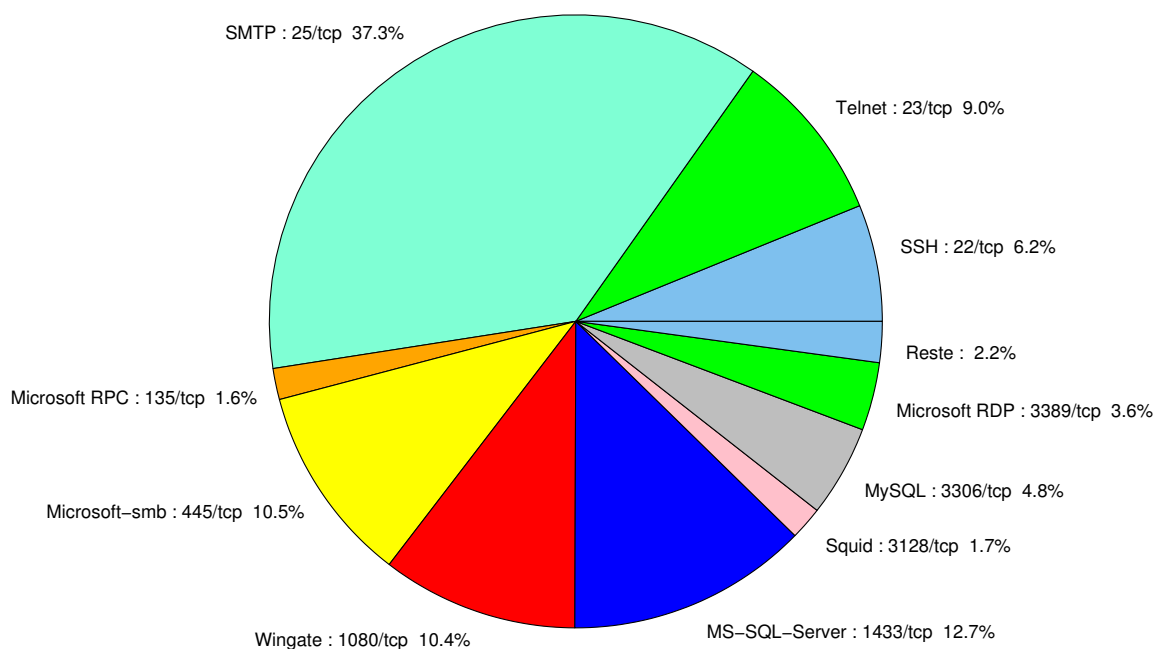


FIG. 1: Répartition relative des ports pour la semaine du 15 au 21 juillet 2011

port	pourcentage
25/tcp	37.26
1433/tcp	12.73
445/tcp	10.47
1080/tcp	10.36
23/tcp	9.03
22/tcp	6.16
3306/tcp	4.82
80/tcp	4.62
3389/tcp	3.59
3128/tcp	1.74
135/tcp	1.64
4899/tcp	0.82
2967/tcp	0.71
21/tcp	0.51
42/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

22 juillet 2011 version initiale.