Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 juillet 2011
N° CERTA-2011-ACT-027

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-27

Gestion du document

Référence	CERTA-2011-ACT-027
Titre	Bulletin d'actualité 2011-27
Date de la première version	08 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-027.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-027/

1 Alerte du CERTA concernant des vulnérabilités dans Apple iOS

Cette semaine, le CERTA a émis une alerte car deux vulnérabilités dans Apple iOS ont été publiées et sont actuellement exploitées.

Utilisées pour débloquer (*jailbreaker*) les iPhones, iPads ou iPods, elles peuvent cependant être également employées à des fins malveillantes. En effet, l'exploitation réussie de ces deux vulnérabilités permet d'exécuter du code arbitraire à distance avec des privilèges élevés, donnant ainsi à l'attaquant le contrôle total de l'appareil.

Les deux vulnérabilités sont similaires à celles découvertes en août 2010 (voir avis CERTA CERTA-2010-380) et peuvent être exploitées au moyen d'un document PDF spécialement conçu. Le CERTA recommande donc la plus grande prudence lors de la navigation et l'utilisation de liens sur des sites, courriels et MMS.

Le CERTA recommande de ne pas procéder au déblocage de son appareil, celui-ci brisant le modèle de sécurité mis en place. De même, l'installation d'applications dont l'origine est peu contrôlée n'est pas recommandée.

Enfin, une vigilance particulière doit être apportée par les responsables de la sécurité informatique quant à l'utilisation de ces appareils dans leur système d'information et à sensibiliser les utilisateurs à l'importance de ne pas traiter d'informations sensibles dessus. S'il s'agit d'appareils professsionnels, les limites d'utilisation doivent être établies.

Documentation

- Alerte CERTA CERTA-2011-ALE-004 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ALE-004/
- Avis CERTA CERTA-2010-380 du 12 Août 2010
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-380/

2 Compromission de vsftpd

Cette semaine, une compromission des sources du serveur `vsftpd` a été mise au jour. En effet, il est apparu que la version 2.3.4 du serveur FTP `vsftpd` disponible sur le serveur principal du projet comportait une porte dérobée. La compromission a pu être détectée simplement en vérifiant la signature `GPG` de l'archive contenant les sources. En effet la signature calculée à partir de l'archive .tar.gz ne correspondait pas au contenu du fichier .asc disponible sur le serveur du projet ou sur les autres miroirs.

Par ailleurs, la porte dérobée n'était pas réellement discrète et a donc pu être rapidement identifiée dans le code source.

Recommandations :

Dans l'hypothèse où vous auriez utilisé les sources de vsftpd version 2.3.4 récemment pour déployer un serveur FTP, il convient de calculer sans délais la signature de l'archive téléchargée et de la comparer avec la signature disponible sur le site de `vsftpd` afin de vous assurer que vous n'utilisez pas la version compromise.

De manière générale et quand cela est possible, il convient de vérifier la signature des logiciels téléchargés sur l'Internet. Ceci ne constitue pas une garantie absolue puisque les signatures ont pu, elles aussi, être altérées mais elles permettent au moins une première vérification.

3 Vulnérabilité dans Bind

Cette semaine, le CERTA a publié l'avis CERTA-2011-AVI-381 relatif à deux vulnérabilités présentes dans le serveur `DNS Bind`. Son éditeur `ISC` qualifie lui-même la première faille (CVE-2011-2464) de sérieuse et invite les utilisateurs du produit à le mettre à jour dans les plus brefs délais. En effet, cette vulnérabilité touche de nombreuses versions réparties dans les branches 9.6, 9.7 et 9.8 de `Bind`. Par ailleurs, un seul paquet suffit à un éventuel attaquant distant pour provoquer un arrêt inopiné du service *named*. Plusieurs distributions ou fournisseurs de systèmes d'exploitation, comme FreeBSD, Debian ou Ubuntu, ont déjà publié une version corrigeant le problème.

Recommandations :

Dans la mesure où le service de nommage `DNS` constitue un élément critique du système d'information ; si celui-ci s'appuie sur `Bind`, il conviendra de mettre à jour dès la publication du correctif pour votre plate-forme.

4 Filtrage Google sur des domaines malveillants

Depuis quelque temps, *Google* n'affiche plus, lors du résultat d'une recherche, des sites appartenant à certains sous-domaines, pour cause d'hébergement de codes malveillants. Le but est d'éviter que les internautes aillent sur un site malveillant après une recherche sur un sujet porteur (par exemple, la mort d'une personne, une catastrophe naturelle, etc.). Il y a quelques semaines, les sites du sous-domaine `cz.cc` ont ainsi été purgés des recherches. C'est désormais au tour de `co.cc` de faire l'objet d'un déréférencement de la part de *Google*.

Cette politique de filtrage n'a qu'une efficacité relative. Elle n'empêche pas les internautes de suivre des liens, et donc de se rendre malgré tout sur des sites malveillants. De plus, les attaquants changent les noms de domaine utilisés, ce qui ne fait que déplacer le problème. Enfin, elle est réellement pénalisante pour ceux possédant un site légitime dans ces sous-domaines.

La politique de filtrage mise en place par *Google* n'est pas clairement définie. Il pourrait donc être possible de provoquer un déréférencement du moteur de recherche *Google* en déployant un grand nombre de codes malveillants, après une intrusion par exemple.

Documentation :

- Message sur le blog sécurité de Google le 17 juin 2011 :
  http://googleonlinesecurity.blogspot.com/2011/06/protecting-users-from-malware-hosted-on.html

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 01 au 07 juillet 2011, le CERTA a émis les avis suivants :

- CERTA-2011-ALE-004 : Vulnérabilités dans Apple iOS
- CERTA-2011-AVI-376 : Vulnérabilités dans Opera
- CERTA-2011-AVI-377 : Vulnérabilité dans Zope et Plone
- CERTA-2011-AVI-378 : Vulnérabilité dans Drupal
- CERTA-2011-AVI-379 : Vulnérabilité dans WordPress
- CERTA-2011-AVI-380 : Multiples vulnérabilités dans phpMyAdmin
- CERTA-2011-AVI-381 : Multiples vulnérabilités dans Bind
- CERTA-2011-AVI-382 : Vulnérabilité dans Cisco Content Services Gateway
- CERTA-2011-AVI-383 : Vulnérabilité dans Qemu

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 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.

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 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.

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.

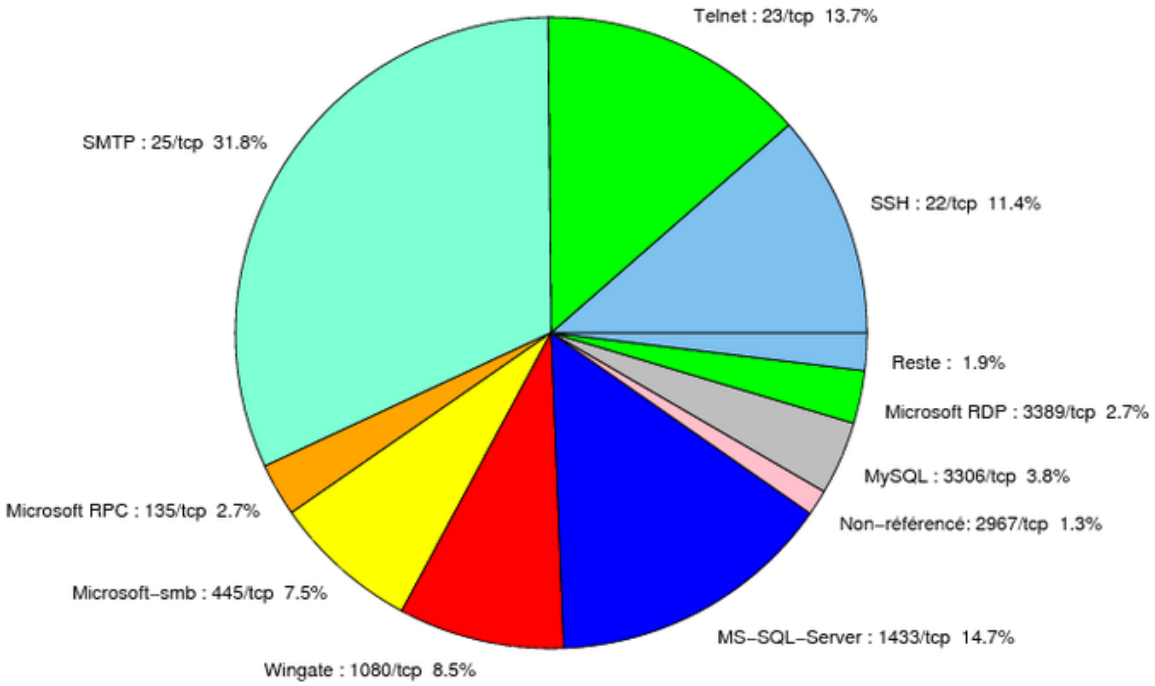

FIG. 1: Répartition relative des ports pour la semaine du 01 au 07 juillet 2011

port	pourcentage
25/tcp	31.79
1433/tcp	14.67
23/tcp	13.71
22/tcp	11.44
1080/tcp	8.47
445/tcp	7.51
3306/tcp	3.75
80/tcp	3.05
3389/tcp	2.7
2967/tcp	1.31
3128/tcp	0.96
4899/tcp	0.52
1434/udp	0.34
143/tcp	0.08

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

08 juillet 2011 version initiale.