Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 août 2011
N° CERTA-2011-ACT-033

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-33

Gestion du document

Référence	CERTA-2011-ACT-033
Titre	Bulletin d'actualité 2011-33
Date de la première version	19 août 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-033.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-033/

1 Mise à jour des produits Mozilla

Cette semaine, *Mozilla* a publié un nombre important de mises à jour pour *Firefox*, *Thunderbird* et *SeaMonkey*. Certaines de ces mises à jour concernent des vulnérabilités jugées critiques par l'éditeur. Elles permettent notamment à une personne malintentionée d'exécuter du code arbitraire à distance. Le CERTA recommande de mettre à jour l'ensemble des produits concernés dans les plus brefs délais.

Documentation

– Bulletins de sécurité *Mozilla* mfsa2011-29 à msfa2011-33 du 16 août 2011 :
http://www.mozilla.org/security/announce/2011/mfsa2011-29.html
http://www.mozilla.org/security/announce/2011/mfsa2011-30.html
http://www.mozilla.org/security/announce/2011/mfsa2011-31.html
http://www.mozilla.org/security/announce/2011/mfsa2011-32.html
http://www.mozilla.org/security/announce/2011/mfsa2011-33.html

2 Fin du support ISC DHCP 3.1

Comme indiqué dans le bulletin de sécurité ISC du 10 août 2011 (avis CERTA-2011-AVI-452), le support de la version *3.1-ESV* de *ISC HCP* arrive à son terme.

Le CERTA recommande donc aux utilisateurs des versions 3.x de planifier le passage en version 4 de ISC DHCP dès que possible.

Documentation

– Avis de sécurité du CERTA CERTA-2011-AVI-452 :
http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-452/index.html

3 Ordiphones et sécurité : le *juicejacking*

Lors de la conférence *Defcon* qui s'est tenue du 4 au 7 août 2011 à Las Vegas, les chercheurs en sécurité informatique Brian Markus, Joseph Mlodzianowski et Robert Rowley ont mené une expérience grandeur nature afin de démontrer la faisabilité d'une nouvelle attaque visant les ordiphones : le *juicejacking*.

Ces trois chercheurs ont installé sur le site de la conférence une borne en libre service permettant de recharger un ordiphone. Les bornes de ce type sont en règle générale installées dans les gares, les aéroports ou tout autre lieu ouvert au public.

Cependant, la borne installée était quelque peu différente des bornes classiques. En effet, au lieu de simplement délivrer de l'énergie afin de recharger l'ordiphone, elle essayait aussi d'établir une connexion vers ce dernier. Ce type de connexion est possible car les ordiphones utilisent souvent un seul et même port pour le rechargement et le transfert de données (mini-usb ou autre). Les chercheurs ont ainsi pu confirmer leur soupçons : la plupart des appareils mobiles qui ont été connectés étaient configurés pour accepter automatiquement les connexions sur ce port.

Il devenait alors possible d'accéder aux données contenues sur le téléphone. Bien entendu, dans certains cas l'accès à ces données était limité voire bloqué. Cependant, il convient de prendre en compte ce type de menace lors de la connexion de son ordiphone sur un équipement non maîtrisé.

Il est possible de se prémunir de ce type d'attaques. En effet, certains téléphones permettent de bloquer toute connexion sur le port de communication ou bien peuvent être configurés pour demander une confirmation avant l'établissement de une connexion. Cependant, si ces options ne sont pas disponibles, il reste toujours possible de se connecter à ces bornes grâce à un cable usb ne transférant que l'énergie et pas les données, bloquant de fait toute connexion extérieure. Bien entendu, la meilleure des solutions reste tout de même de n'utiliser que son chargeur secteur personnel.

Documentation

– Researchers warn of jucejacking threat :
http://www.thinq.co.uk/2011/8/19/researchers-warn-juicejacking-threat/

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 12 août au 18 août 2011, le CERTA a émis les publications suivantes :

– CERTA-2011-AVI-453 : Vulnérabilités dans McAfee SaaS Endpoint Protection
– CERTA-2011-AVI-454 : Vulnérabilités dans Apache Tomcat
– CERTA-2011-AVI-455 : Vulnérabilités dans Symantec Veritas Enterprise Administrator
– CERTA-2011-AVI-456 : Vulnérabilité dans CA ARCserve D2D
– CERTA-2011-AVI-457 : Vulnérabilités dans différents produits Mozilla
– CERTA-2011-AVI-458 : Multiples vulnérabilités dans RealPlayer
– CERTA-2011-AVI-459 : Multiples vulnérabilités dans Ruby on Rails

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

– CERTA-2011-AVI-429-001 : Vulnérabilités dans Apple QuickTime (ajout de références CVE)
– CERTA-2011-AVI-452-001 : Vulnérabilités dans ISC DHCP (ajout des références aux bulletins Debian, Red Hat et Ubuntu)

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.

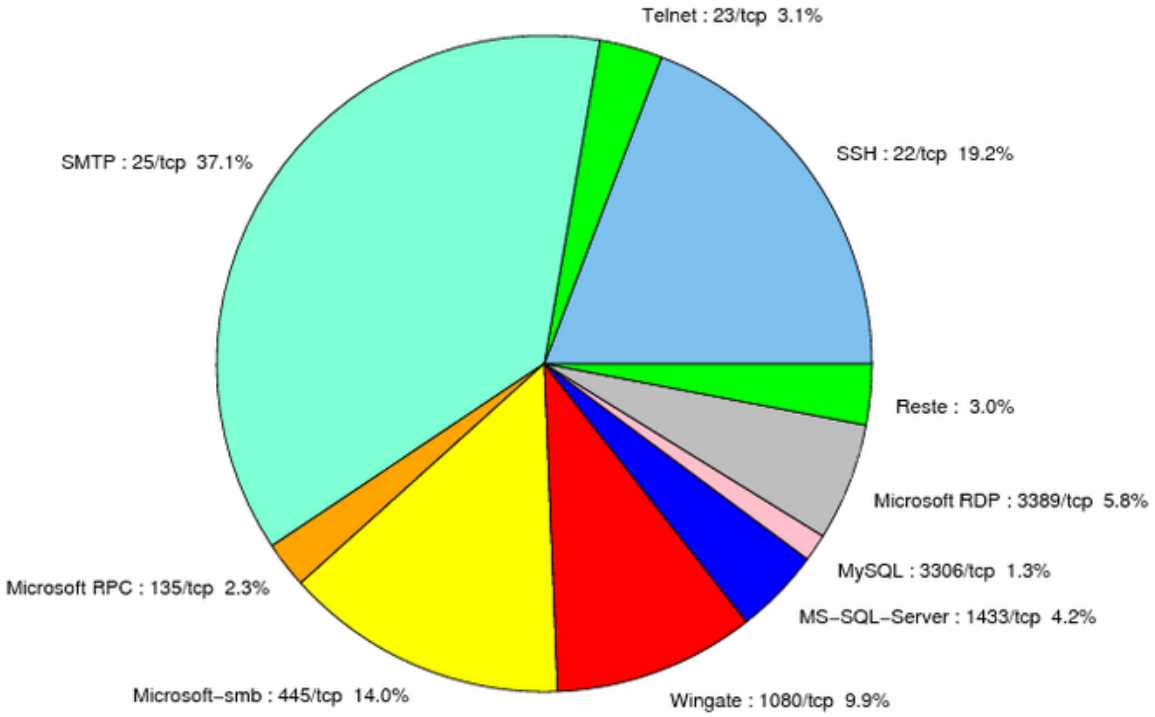

FIG. 1: Répartition relative des ports pour la semaine du 12 au 18 août 2011

port	pourcentage
25/tcp	37.09
22/tcp	19.17
445/tcp	13.98
1080/tcp	9.94
3389/tcp	5.8
1433/tcp	4.24
23/tcp	3.31
80/tcp	2.9
135/tcp	2.27
3306/tcp	1.34
2967/tcp	0.82
4899/tcp	0.72
21/tcp	0.62
3127/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

19 août 2011 version initiale.