

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-34

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-034>

Gestion du document

Référence	CERTA-2011-ACT-034
Titre	Bulletin d'actualité 2011-34
Date de la première version	26 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-034.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-034/>

1 Incidents de la semaine

Cette semaine, le CERTA a traité un incident concernant la compromission d'un poste de travail. L'analyse du disque dur a permis de montrer que l'infection du poste a eu lieu suite à la visite d'un site Internet compromis. Ce dernier redirigeait les visiteurs en fonction du *User-Agent* et du *referrer*, et ce lors de la première visite uniquement. La redirection n'affectait que les internautes utilisant Microsoft Windows et ayant suivi un lien depuis un moteur de recherche. Le téléchargement d'un code malveillant leur était alors proposé. Ce code malveillant était nommé en fonction de la recherche effectuée, pour inciter l'utilisateur à ouvrir le fichier. Par exemple, une recherche de la chaîne « toto » aurait donné un fichier nommé « toto.com ».

On peut facilement imaginer d'autres cas, plus dangereux, où l'utilisateur ne doit pas ouvrir un fichier mais est redirigé vers un site exploitant une vulnérabilité. Cet incident montre une nouvelle fois qu'on ne peut se fier aux sites que l'on visite, même connus, puisque ceux-ci peuvent être compromis.

Recommandations :

Il n'est pas aisé de se prémunir des incidents de ce type. Néanmoins, l'un des mécanismes de l'attaque reposant sur l'analyse du *referrer*, il est possible d'éviter la redirection vers le site malveillant soit :

- en saisissant manuellement les adresses que l'on veut visiter ;
- soit en copiant puis collant les résultats donnés par le moteur de recherche.

2 Dénis de service dans Apache

Des scripts, librement disponibles sur l'Internet depuis cette semaine, permettent de provoquer un déni de service distant sur Apache (versions 1.3.x et 2.x) en utilisant une vulnérabilité de type épuisement de mémoire.

Pour ce faire, ces scripts envoient des requêtes HTTP de type HEAD spécialement conçues employant notamment l'entête *HTTP Range* et attendant un retour compressé au format *gzip*. Ce champ permet de demander une partie (intervalle) de la réponse. Son utilité principale est de permettre le téléchargement partiel de fichiers volumineux. Afin de provoquer un déni de service, les scripts vont demander un nombre élevé d'intervalles se chevauchant à l'aide du champ *Range*. L'utilisation d'un nombre élevé d'intervalles va entraîner l'épuisement de la mémoire.

L'équipe Apache a réagi à cette menace en proposant un certain nombre de contre-mesures. Elle propose notamment d'utiliser *mod_headers* pour supprimer le champ *Range* des requêtes entrantes à l'aide de la directive suivante : *RequestHeader unset Range*. D'autres contre-mesures sont proposées sur la liste de diffusion *apache-httpd-dev*. Il est également envisageable de contrôler la présence du champ *Range* à l'aide d'un proxy inverse ou d'un firewall applicatif.

L'équipe Apache prévoit de sortir rapidement un correctif pour cette vulnérabilité. Il faut noter que la version 1.3 de Apache ne sera pas corrigée car elle n'est plus maintenue. Le CERTA recommande la mise en place rapide du correctif lorsqu'il sera disponible.

Documentation

- Discussion sur la liste de diffusion *apache-httpd-dev* :
<http://marc.info/?l=apache-httpd-dev&m=131418828705324&w=2>

3 Mise à jour 5.3.8 de PHP

Cette semaine, le CERTA a publié un avis concernant une mise à jour de sécurité de PHP (avis CERTA-2011-AVI-461). Cette version, 5.3.7, corrige plusieurs vulnérabilités mais apporte également deux régressions :

- une régression dans la fonction *crypt()* lorsque celle-ci est utilisée pour créer un condensat MD5 (seul le « sel » est retourné) ;
- une régression dans les connexions SSL effectuées par le pilote MySQL *mysqlnd*.

Une nouvelle version, 5.3.8, a donc été publiée afin de supprimer ces régressions.

Le CERTA recommande d'effectuer la mise à jour de PHP vers la version 5.3.8. Il est à noter également que la branche 5.2 de PHP n'est plus maintenue.

Documentation

- Avis CERTA-2011-AVI-461 du 26 juillet 2011 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-461/>
- Mise en garde sur la version PHP 5.3.7 du 22 août 2011 :
<http://www.php.net/archive/2011.php#id2011-08-22-1>
- Annonce de la version PHP 5.3.8 du 23 août 2011 :
<http://www.php.net/archive/2011.php#id2011-08-23-1>

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 19 au 25 août 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-460 : Vulnérabilités dans OTRS
- CERTA-2011-AVI-462 : Vulnérabilité dans EMC RSA Adaptive Authentication On-Premise
- CERTA-2011-AVI-463 : Vulnérabilité dans IBM Websphere Service Registry and Repository
- CERTA-2011-AVI-464 : Multiples vulnérabilités dans Google Chrome
- CERTA-2011-AVI-465 : Vulnérabilité dans stunnel
- CERTA-2011-AVI-466 : Vulnérabilités dans Pidgin
- CERTA-2011-AVI-467 : Multiples vulnérabilités dans EMC AutoStart
- CERTA-2011-AVI-468 : Vulnérabilité dans Citrix Access Gateway
- CERTA-2011-AVI-469 : Vulnérabilité dans Cisco IOS
- CERTA-2011-AVI-470 : Vulnérabilité dans Cisco IOS
- CERTA-2011-AVI-471 : Vulnérabilité dans les produits F-Secure
- CERTA-2011-AVI-472 : Vulnérabilité dans HP Easy Printer Care

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

- CERTA-2011-AVI-316-001 : Vulnérabilité dans Dovecot (ajout des références aux bulletins Debian, Fedora, Mandriva, RedHat, Suse et Ubuntu)
- CERTA-2011-AVI-416-001 : Vulnérabilités dans Samba (SWAT) (ajout des références aux bulletins Debian, Mandriva et Ubuntu)
- CERTA-2011-AVI-457-001 : Vulnérabilités dans différents produits Mozilla et dérivés (ajout des dérivés Debian (iceape, icedove, iceweasel))
- CERTA-2011-AVI-459-001 : Multiples vulnérabilités dans Ruby on Rails (ajout des références CVE)
- CERTA-2011-AVI-461-001 : Vulnérabilités dans PHP (ajout du correctif de la version 53.8 du 23 août 2011.)

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 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.

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 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.

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.

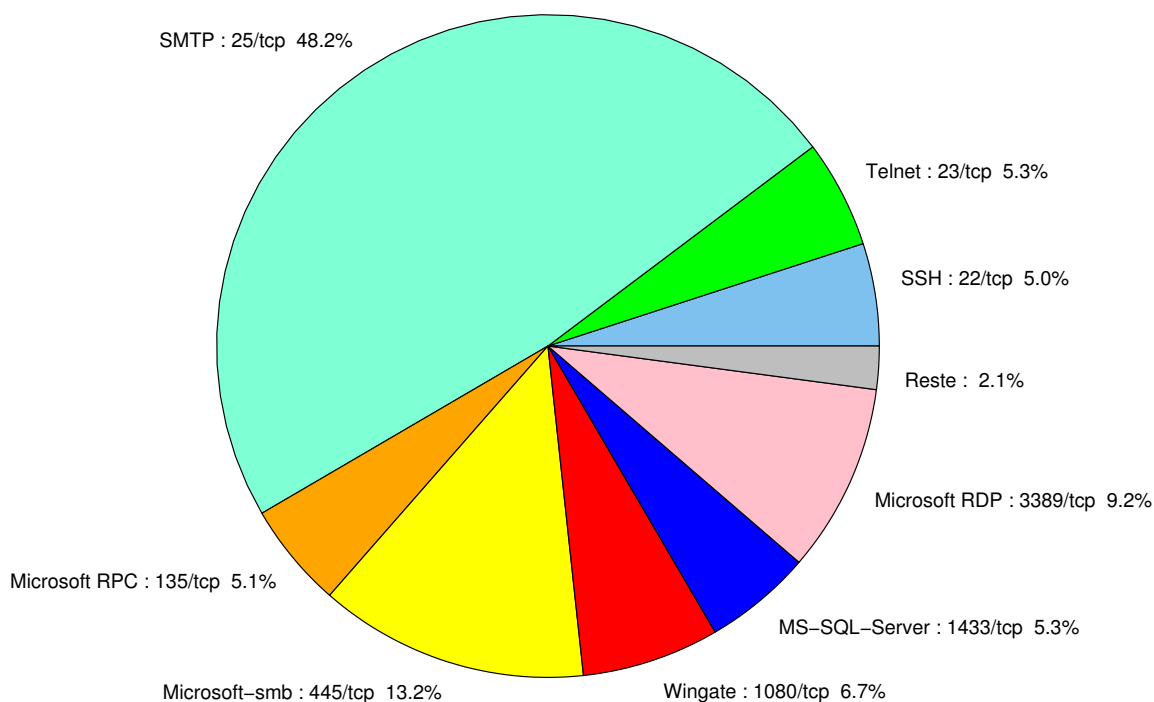


FIG. 1: Répartition relative des ports pour la semaine du 19 au 25 août 2011

port	pourcentage
25/tcp	48.15
445/tcp	13.15
3389/tcp	9.6
1080/tcp	6.71
1433/tcp	5.26
135/tcp	5.13
22/tcp	5
80/tcp	1.97
4899/tcp	0.78
3306/tcp	0.52
3128/tcp	0.26
2967/tcp	0.13

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

26 août 2011 version initiale.