Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 août 2011
N° CERTA-2011-ACT-032

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-32

Gestion du document

Référence	CERTA-2011-ACT-032
Titre	Bulletin d'actualité 2011-32
Date de la première version	12 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-032.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-032/

1 Mise à jour Microsoft du mois d'août

Cette semaine, `Microsoft` a publié treize bulletins de sécurité pour ses produits. Parmi ces bulletins, quatre traitent de vulnérabilités permettant l'exécution de code arbitraire à distance et deux sont classés comme critiques par l'éditeur.

Les deux bulletins critiques sont :
– le bulletin MS11-057 qui corrige sept vulnérabilités dans `Internet Explorer` ;
– le bulletin MS11-058 qui corrige deux vulnérabilités dans le serveur `Windows DNS`.

Le CERTA rapelle qu'il est nécessaire d'appliquer l'ensemble de ces mises à jour de sécurité dès que possible.

Documentation

– Résumé du bulletin de sécurité Microsoft de juin 2011 :
http://www.microsoft.com/france/technet/security/bulletin/ms11-aug.mspx

2 Mise à jour Adobe

Adobe a publié cette semaine cinq bulletins de sécurité concernant les produits suivants :

- Adobe Shockwave Player ;
- Adobe Flash Media Server ;
- Adobe Flash Player ;
- Adobe Photoshop CS5 ;

Les vulnérabilités concernant Adobe Shockwave Player, Adobe Flash Player et Adobe Photoshop CS5 permettent l'exécution de code arbitraire à distance. Il est impératif d'appliquer les mises à jour dès que possible.

Documentation

- Avis de sécurité du CERTA CERTA-2011-AVI-446 du 10 août 2011 : http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-446/index.html
- Avis de sécurité du CERTA CERTA-2011-AVI-447 du 10 août 2011 : http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-447/index.html
- Avis de sécurité du CERTA CERTA-2011-AVI-448 du 10 août 2011 : http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-448/index.html
- Avis de sécurité du CERTA CERTA-2011-AVI-449 du 10 août 2011 : http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-449/index.html

3 Des fichiers temporaires qui peuvent en dire beaucoup

Il est de temps en temps nécessaire à l'administrateur d'un serveur ou à un webmestre d'éditer un fichier, parfois dans l'urgence, d'un service en production. Que ce soit un fichier de configuration ou un simple élément d'une feuille de style, la modification de ces fichiers passe par un éditeur de texte, plus ou moins évolué, en ligne de commande ou utilisant une interface graphique.

Or la plupart de ces logiciels ont recours à des fichiers temporaires, ou à des fichiers de sauvegarde. Un éditeur en ligne de commande comme vim va, lors de l'ouverture et de l'édition d'un fichier « test.html », créer un fichier temporaire, dans le même dossier que l'original. Ce fichier, nommé « .test.html.swp » dans notre exemple, joue le rôle de verrou exclusif (évitant ainsi l'édition simultanée du fichier original) ainsi que d'historique des modifications apportées à « test.html ». En cas de fermeture inopinée de l'éditeur, ce fichier peut ne pas être supprimé. vim crée également un fichier de sauvegarde, dont le nom est « test.html~» et qui est une copie du fichier « test.html », dans son état avant édition. L'éditeur emacs a un comportement similaire, mais les fichiers temporaires sont alors de la forme « #test.html# ».

Au delà de la multiplication dans une arborescence des fichiers de sauvegarde du type « test.html~», ce comportement peut poser des problèmes de sécurité. En effet, imaginons un fichier « database.php », fournissant à tout script *PHP* qui en fera l'inclusion une liste de fonctions et d'indentifiants requis pour accéder à une base de données. Si un administrateur édite ce fichier, une copie « database.php~» apparaîtra dans le même dossier que le script « database.php ». Ce fichier, avec l'extension « .php~» ne sera pas interprété par le serveur Web comme un fichier PHP mais sera servi au client comme un fichier texte, c'est-à-dire en envoyant son contenu brut, et donc les identifiants qu'il contient.

Ce scénario montre qu'il est indispensable de connaître le comportement de chacun des outils utilisés sur un serveur de production. Les manuels des éditeurs de texte indiquent les moyens de désactiver la création de fichiers temporaires et de sauvegarde, ou encore de les créer systématiquement dans un autre dossier de l'arborescence. Une autre possibilité est de configurer les différents services (Web, partage de fichiers, . . .) afin qu'ils ignorent ces fichiers.

4 Internet et vie privée

Il existe un grand nombre de technologies liées à l'Internet qui permettent à une société de suivre les activités d'un internaute afin, par exemple, de lui proposer de la publicité ciblée. Parmis celles-ci, les plus connues sont sans aucun doute les *cookies* HTTP et leurs homologues *Flash*. L'avénement de HTML5 apporte aussi son lot de nouveautés dans ce domaine avec les technologies de type *Web Storage* (*cf.* bulletin d'actualité 2011-30).

Une nouvelle méthode vient s'ajouter à cette liste. Il ne s'agit pas d'une nouvelle technologie mais plutôt du détournement d'un mécanisme déjà existant : les *ETags*.

4.1 Qu'est-ce qu'un ETag?

Un *Etag* ou plus précisément un *HTTP ETag* est un code d'identification associé à une ressource par un serveur Web.

Ce code est utilisé par le mécanisme de cache Web. Lors de l'accès initial à une ressource par un client, le serveur Web renvoie au navigateur la ressource qu'il a demandée et également un *ETag* identifiant ces données. Cet *ETag* est ensuite renvoyé par le client à chaque accès à la ressource. Si l'*ETag* envoyé correspond à la ressource demandée, le serveur signifie au client qu'il peut utiliser la version de la ressource dont il dispose dans son cache local. Dans le cas contraire, la ressource modifiée et un nouvel *ETag* identifiant cette dernière sont envoyés.

4.2 Suivi par ETag

Certains sites Web détournent le mécanisme de cache afin d'assurer le suivi des clients qui les contactent. Le principe est simple : lors de l'accès à une ressource particulière, un *ETag* propre au client, et non à la ressource, est généré et est retourné avec la ressource au client. Quand ce dernier voudra accéder de nouveau à cette donnée, son navigateur présentera l'*ETag* qui y est associé au serveur. Le serveur n'a alors plus qu'à comparer cet *Etag* avec la liste de ceux qu'il a distribués pour identifier le client.

Afin de limiter les effets de ce suivi, il est recommandé de vider régulièrement le cache de son navigateur Web. Il est aussi possible, sur certains navigateurs, de réduire la taille du cache local à 0. Cependant, ce type de configuration à un impact négatif sur la vitesse de navigation : il faut télécharger l'ensemble des données à chaque accès à une ressource.

Documentation

- Flash cookies and privacy II :
  http://www.techpolicy.com/FlashCookiesPrivacyII.aspx
- HTTP ETag :
  http://en.wikipedia.org/wiki/HTTP_ETag
- Bulletin d'actualité 2011-30 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-030/index.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 04 août au 11 août 2011, le CERTA a émis les publications suivantes :

– CERTA-2011-AVI-430 : Multiples vulnérabilités dans Bugzilla
– CERTA-2011-AVI-431 : Vulnérabilités dans Moodle
– CERTA-2011-AVI-432 : Multiples vulnérabilités dans TYPO3
– CERTA-2011-AVI-433 : Multiples vulnérabilités dans Internet Explorer
– CERTA-2011-AVI-434 : Vulnérabilités dans le serveur Windows DNS
– CERTA-2011-AVI-435 : Vulnérabilité dans Data Access Components
– CERTA-2011-AVI-436 : Vulnérabilités dans Microsoft Visio
– CERTA-2011-AVI-437 : Vulnérabilité dans le service d'accès au bureau à distance Windows par le Web
– CERTA-2011-AVI-438 : Vulnérabilité dans le pilote NDISTAPI du service d'accès à distance de Microsoft
– CERTA-2011-AVI-439 : Vulnérabilité dans le processus CSRSS de Microsoft Windows
– CERTA-2011-AVI-440 : Vulnérabilités dans la pile TCP/IP de Microsoft Windows
– CERTA-2011-AVI-441 : Vulnérabilité dans la protocole RDP de Microsoft Windows
– CERTA-2011-AVI-442 : Vulnérabilité dans les contrôles Chart ASPNET de Microsoft
– CERTA-2011-AVI-443 : Vulnérabilité dans Microsoft Report Viewer
– CERTA-2011-AVI-444 : Vulnérabilité dans le noyau Windows
– CERTA-2011-AVI-445 : Vulnérabilité dans Microsoft NET Framework
– CERTA-2011-AVI-446 : Multiples vulnérabilités dans Adobe Shockwave Player
– CERTA-2011-AVI-447 : Vulnérabilité dans Adobe Flash Media Server
– CERTA-2011-AVI-448 : Multiples vulnérabilités dans Adobe Flash Player
– CERTA-2011-AVI-449 : Vulnérabilité dans Adobe Photoshop CS5
– CERTA-2011-AVI-450 : Multiples vulnérabilités dans BlackBerry Enterprise Server
– CERTA-2011-AVI-451 : Vulnérabilités dans Symantec Endpoint Protection Manager
– CERTA-2011-AVI-452 : Vulnérabilités dans ISC DHCP

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.

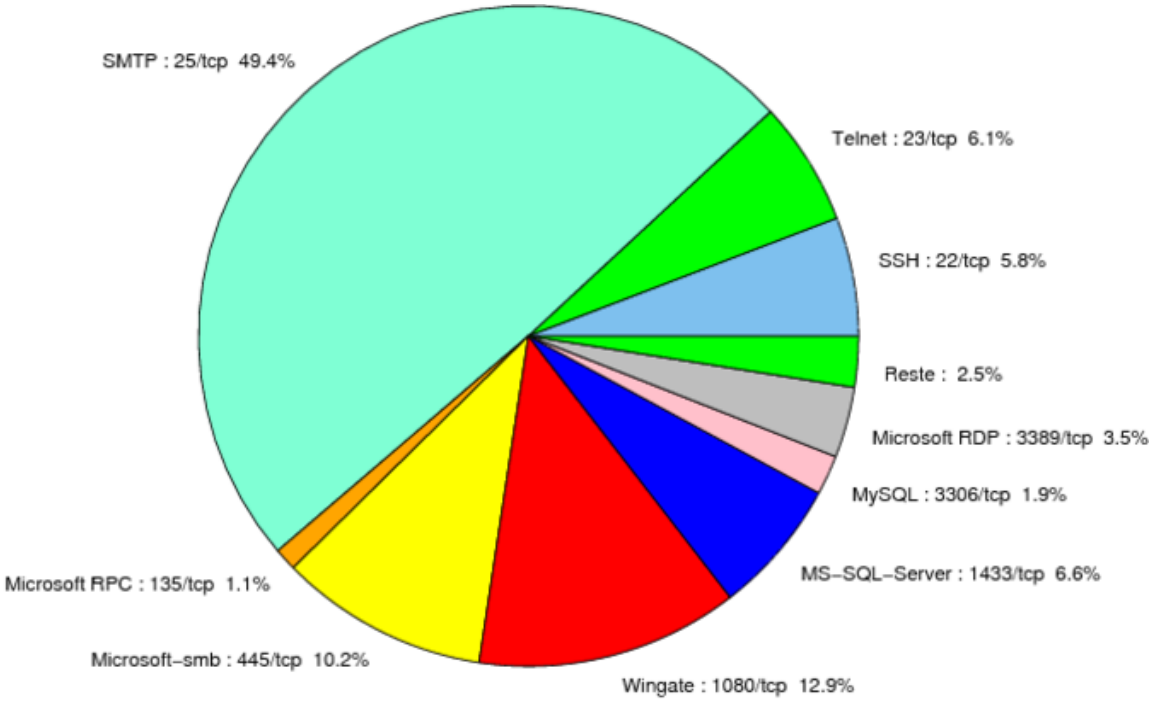

FIG. 1: Répartition relative des ports pour la semaine du 04 au 11 août 2011

port	pourcentage
25/tcp	49.37
1080/tcp	12.86
445/tcp	10.23
1433/tcp	6.63
23/tcp	6.08
22/tcp	5.8
3389/tcp	3.45
80/tcp	2.62
3306/tcp	1.93
3127/tcp	1.24
135/tcp	1.1
4899/tcp	0.82
42/tcp	0.27
2967/tcp	0.13

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

12 août 2011 version initiale.