

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-38

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-2010-ACT-038>

Gestion du document

Référence	CERTA-2010-ACT-038
Titre	Bulletin d'actualité 2010-38
Date de la première version	24 septembre 2010
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-2010-ACT-038.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-2010-ACT-038/>

1 Fuite d'information des applications ASP.NET

Microsoft a publié cette semaine un bulletin de sécurité à propos d'une vulnérabilité non corrigée dans *ASP.NET* permettant le vol d'informations par des utilisateurs malveillants sur certaines applications *ASP.NET*. Parmi les informations pouvant être récupérées de façon illicite, on distingue les fichiers *web.config* qui contiennent souvent des données sensibles comme les informations de session et d'authentification, par exemple les identifiants pour accéder au serveur *MS-SQL Server*. Cette vulnérabilité permet aussi d'accéder à certaines données chiffrées envoyées aux clients, l'attaque est basée sur le principe des oracles cryptographiques, et prend donc un certain temps.

Un moyen de contournement pour se protéger de cette vulnérabilité est d'activer la balise `<customErrors>` et de configurer les applications pour toujours renvoyer la même page d'erreur, quelque soit la nature de l'erreur, en utilisant par exemple l'attribut `defaultRedirect` de la balise. Les moyens de contournement sont précisés dans le bulletin de sécurité Microsoft dont l'adresse est indiquée ci-dessous.

A noter que cette vulnérabilité est actuellement exploitée sur l'Internet.

Documentation

- Bulletin de sécurité Microsoft #2416728 du 17 septembre 2010 :
<http://www.microsoft.com/technet/security/advisory/2416728.mspx>

2 Mise à jour Adobe Flash Player

Cette semaine, une nouvelle version d'Adobe Flash Player a été publiée par l'éditeur. Cette mise à jour corrige la vulnérabilité qui a fait l'objet de l'alerte CERTA-2010-ALE-015. Pour rappel, cette faille permet l'exécution de code arbitraire à distance par une personne malintentionnée.

Cette vulnérabilité est exploitée sur l'Internet, le CERTA recommande donc de déployer rapidement ce correctif disponible pour toutes les plateformes supportées. Une mise à jour du lecteur de fichier PDF d'Adobe est prévue durant la semaine du 04 octobre, le lecteur reste donc pour l'instant vulnérable.

Documentation

- Bulletin de sécurité Adobe APSB10-22 du 20 septembre 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-22.html>
- Alerte CERTA-2010-ALE-015 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-015/>
- Avis CERTA-2010-AVI-447 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-447/>

3 Identification de machine via du code JavaScript

Cette semaine, a été publiée sur l'Internet la dernière version d'une API (Application Programming Interface) en JavaScript permettant la création de cookies particuliers rendant leur effacement difficile par un utilisateur non-averti. En effet, plutôt que d'utiliser les fonctions standards des navigateurs pour créer des cookies normaux, cette API propose d'engendrer un certain nombre de marqueurs spécifiques à différents endroits du navigateur afin de rendre plus persistante l'identification d'une machine. Ainsi, selon l'auteur, il est possible de poser des marqueurs :

- dans le magasin de cookies standard ;
- dans le *Local Shared Objects* qui sert à stocker les cookies pour les objets Flash ;
- dans des images au format PNG créées à la volée par certaines fonctionnalités du langage HTML5 ;
- dans les entrées de l'historique ;
- lors du stockage des ETags HTTP ;
- dans le conteneur `userData` d'Internet Explorer ;
- dans différents magasins de stockage nécessaires au fonctionnement de HTML5 dans le navigateur : *Session*, *Local*, *Global*, *Database*.

Il est ainsi possible de rendre persistant un certain nombre de marqueurs ou cookies malgré les précautions de base qu'aurait pu prendre l'utilisateur du navigateur, et ce, entièrement à son insu.

Recommandations :

L'API détaillée ci-dessus est librement disponible en source ouverte sur l'Internet. Pour qu'elle fonctionne correctement sur le navigateur du client, il est toujours nécessaire que le navigateur supporte les JavaScripts et parfois le langage HTML5. Dans un contexte de confidentialité accrue, il conviendra donc, comme à l'habitude, de désactiver par défaut le support des codes JavaScript par le navigateur.

4 XSS sur Twitter, une régression grand public

Cette semaine un incident de sécurité touchant les utilisateurs du site social de *microblogging* Twitter a largement été médiatisé. Il s'agissait d'une vulnérabilité permettant une attaque en injection de code indirecte (Cf. Documentation). Ce qui est remarquable ici est que cette faille avait déjà été corrigée le mois dernier, il s'agit donc d'une *régression*. Dans le contexte du développement de logiciel, ce terme désigne un retour en arrière sur des

corrections apportées. Il est souvent dû à une erreur de choix des versions des parties utilisées pour construire le produit dans sa globalité.

Cet incident met en avant le problème de l'évolution du niveau de confiance dans le temps. Que cela soit un site Internet ou une application, le cas de *Twitter* illustre bien que le niveau de sécurité peut fortement évoluer dans le temps. La confiance par défaut est donc à proscrire. Il convient de rester vigilant et attentif en toutes circonstances, et pour cela, il est important de bien connaître les sites ou logiciels utilisés afin de percevoir les changements.

Documentation

- Définition provenant de securite-informatique.gouv.fr :
Injection de code indirecte (Cross Site Scripting, CSS, XSS) : Activité malveillante qui consiste à injecter des données arbitraires dans le code de pages HTML. Un utilisateur malveillant peut faire afficher à un site web vulnérable un contenu agressif ; ce contenu peut rediriger l'utilisateur vers d'autres sites, ou transmettre des informations (jetons de sessions, aussi appelés cookies, etc) ou des droits.
- Explications et excuses officielles de Twitter :
<http://blog.twitter.com/2010/09/all-about-onmouseover-incident.html>

5 Un annonceur de publicités malveillantes

Le 19 et 20 septembre 2010, un grand nombre de sites Web malaisiens et indonésiens ont été listés comme potentiellement dangereux par *Google*, suite à la présence de code malveillant sur la plupart de leurs pages.

Le code malveillant se situait en fait dans les bandeaux publicitaires affichés à partir du serveur d'un fournisseur de bannières de publicité.

Le problème a pu être remonté à un annonceur particulier dont le serveur *OpenX* a été compromis, ce qui a permis à l'attaquant de placer le code malveillant au sein des bannières qui y sont hébergées. Celles-ci ont ensuite été transmises au fournisseur de publicité, puis intégrées de manière transparente sur les sites Web des clients.

Bien que ce type d'attaque ne soit pas nouveau, il est intéressant de noter ici le nombre de sites Web qu'il est possible de compromettre rapidement à partir d'une seule attaque réussie. Il convient bien évidemment d'être extrêmement vigilant lorsque du contenu extérieur est inséré automatiquement dans une page de son site.

Documentation

- Article F-Secure :
<http://www.f-secure.com/weblog/archives/00002033.html>

6 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/>

7 Rappel des avis émis

Dans la période du 17 au 23 septembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-441 : Vulnérabilités dans QuickTime
- CERTA-2010-AVI-442 : Vulnérabilité dans IBM Lotus Sametime
- CERTA-2010-AVI-444 : Vulnérabilité dans 3Com OfficeConnect Gigabit VPN Firewall
- CERTA-2010-AVI-445 : Vulnérabilités dans Splunk 41.5
- CERTA-2010-AVI-446 : Multiples vulnérabilités dans IBM WebSphere Application Server Community Edition
- CERTA-2010-AVI-447 : Vulnérabilité dans Adobe Flash Player
- CERTA-2010-AVI-448 : Vulnérabilité dans Mac OS X
- CERTA-2010-AVI-449 : Vulnérabilité dans bzip2
- CERTA-2010-AVI-450 : Vulnérabilité dans 7-zip
- CERTA-2010-AVI-451 : Multiples vulnérabilités dans Plesk Sitebuilder
- CERTA-2010-AVI-452 : Vulnérabilité dans RSA Authentication Agent
- CERTA-2010-AVI-453 : Vulnérabilité des produits Alcatel-Lucent OmniVista 4760
- CERTA-2010-AVI-454 : Vulnérabilités dans Alcatel-Lucent OmniTouch Contact Center Standard Edition
- CERTA-2010-AVI-455 : Vulnérabilité dans Cisco Unified Communications Manager

Durant la même période, les avis suivants ont été mis à jour :

- CERTA-2010-AVI-429-001 : Vulnérabilité dans Samba (ajout de la référence au bulletin Debian)
- CERTA-2010-AVI-443-001 : Vulnérabilités dans IBM DB2 (ajout des références CVE)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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_rubrique67.html

9 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.

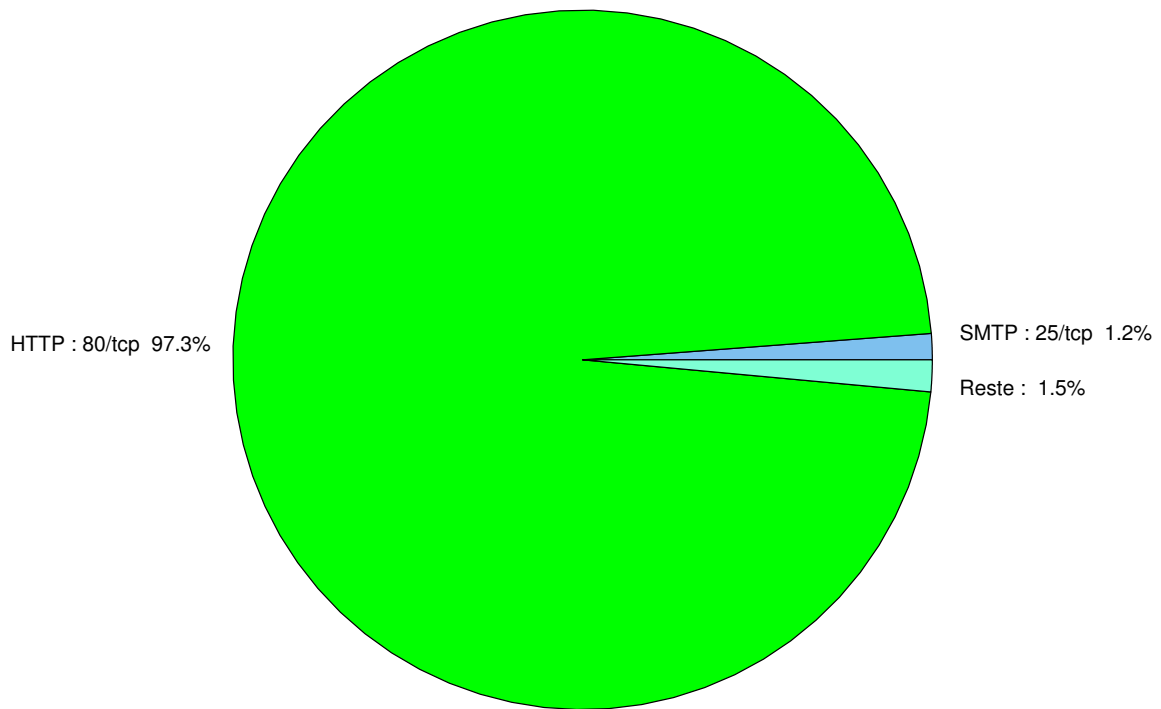


FIG. 1: Répartition relative des ports pour la semaine du 17 au 23 septembre 2010

port	pourcentage
80/tcp	97.44
25/tcp	1.2
1433/tcp	0.23
22/tcp	0.17
2967/tcp	0.16
23/tcp	0.15
135/tcp	0.13
1080/tcp	0.12
3389/tcp	0.1
3306/tcp	0.07
3128/tcp	0.06
1434/udp	0.05
21/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

24 septembre 2010 version initiale.