

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-44

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-044>

Gestion du document

Référence	CERTA-2010-ACT-044
Titre	Bulletin d'actualité 2010-44
Date de la première version	05 novembre 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-044.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-044/>

1 Alerte de la semaine

Cette semaine, le CERTA a publié un bulletin d'alerte (CERTA-2010-ALE-019) concernant une vulnérabilité non corrigée dans Microsoft Internet Explorer. Celle-ci permet l'exécution de code arbitraire à distance via une page *web* spécialement construite, en exploitant une erreur dans certaines séquences CSS où il est possible d'utiliser un objet après son déréférencement.

Du code malveillant exploitant cette faille est d'ores et déjà diffusé sur l'Internet.

Dans l'attente de la publication du correctif par l'éditeur, le CERTA recommande l'application des procédures de contournement provisoire détaillées dans le bulletin d'alerte CERTA-2010-ALE-019.

Documentation

– Alerte CERTA-2010-ALE-019 :

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-019>

2 Incidents de la semaine

Le CERTA a traité cette semaine plusieurs cas de défiguration pour lesquels le scénario d'attaque était systématiquement le même. L'attaquant a recherché des scripts permettant le dépôt de fichier. Lorsqu'il en trouvait, il l'utilisait pour installer une porte dérobée écrite en PHP (*phpshell*), cette dernière lui permettant de réaliser, parmi d'autres actions, une défiguration. En particulier, l'attaquant a utilisé *FCKeditor* pour le dépôt de ses fichiers.

Le logiciel *FCKeditor*, désormais appelé *CKEditor*, est un éditeur de texte qui peut être utilisé pour des pages Web. Il est directement intégré dans certains gestionnaires de contenu. Il est doté d'une fonctionnalité de dépôt de fichiers qui peut être détournée par un attaquant en vue d'installer des outils d'attaque.

Le CERTA recommande donc, outre le déploiement des mises à jour, de mettre en place des restrictions d'accès à tout logiciel de dépôt de fichiers.

3 Retour sur les vulnérabilités Adobe

La semaine dernière, le CERTA a publié une alerte concernant Adobe Flash Player, Adobe Reader et Acrobat (CERTA-2010-ALE-018). En effet, une vulnérabilité critique affecte ces produits et permet à une personne malintentionnée d'exécuter du code arbitraire à distance.

Cette semaine, Adobe a annoncé la mise à disposition d'un correctif pour Adobe Flash Player pour Windows, Macintosh, Linux et Solaris (cf. CERTA-2010-AVI-538). Il est donc impératif de mettre à jour Adobe Flash Player à la version 10.1.102.64.

Cependant, nous rappelons qu'Adobe n'a pas publié de correctif concernant les produits suivants :

- Adobe Reader 9.4 ;
- Adobe Acrobat 9.4.

De ce fait, la mise en place des actions suivantes est toujours fortement recommandée :

- supprimer ou interdire l'accès au composant *authplay.dll* (cette action bloque l'exécution de contenu Flash et provoque une erreur à l'ouverture d'un document *PDF* contenant du Flash) ;
- utiliser un logiciel alternatif.

Documentation

- Bulletin de sécurité Adobe APSA10-05 du 28 octobre 2010 :
<http://www.adobe.com/support/security/advisories/apsa10-05.html>
- Alerte CERTA-2010-ALE-018
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-018>
- Bulletin de sécurité Adobe APSB10-26 du 04 novembre 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-26.html>
- Avis CERTA-2010-AVI-538
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-538>

4 EMET version 2

Il y a quelques semaines Microsoft a publié la version 2 de son outil EMET. Pour mémoire, cet utilitaire avait fait l'objet d'un article dans le bulletin d'actualité CERTA-2009-ACT-044. Cette nouvelle version reprend le mode de fonctionnement de la précédente et se compose d'une bibliothèque de fonctions et d'un programme en ligne de commande permettant de le configurer. Chose nouvelle, il est désormais possible d'effectuer cette configuration via une interface graphique rendant plus convivial le paramétrage sur de multiples applications différentes. Nous ne détaillerons pas à nouveau les fonctionnalités déjà présentes dans la version 1 mais nous pourrions nous attarder sur celles apparues dans cette deuxième mouture :

- le Mandatory ASLR donne la possibilité de forcer l'allocation de mémoire de façon non-linéaire (*randomization*) quelles que soient les options de compilation initiale du programme ;
- l'Export Address Table Access Filtering ou EAF permet d'empêcher un code malveillant d'utiliser facilement l'API (Application Programming Interface) de Windows afin de s'exécuter correctement.

Comme pour la première version, il conviendra de bien tester l'impact d'EMET sur une application donnée avant de le déployer en production. De plus, en fonction de la version de Microsoft Windows utilisée, les fonctionnalités proposées ne seront pas forcément effectives. Typiquement, l'activation de l'ASLR sera impossible sous Windows XP SP3.

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 29 octobre au 04 novembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-522 : Vulnérabilité dans IBM WebSphere
- CERTA-2010-AVI-523 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2010-AVI-524 : Vulnérabilité dans PAM
- CERTA-2010-AVI-525 : Vulnérabilités dans Symantec IM Manager
- CERTA-2010-AVI-526 : Multiples vulnérabilités dans IBM HTTP Server
- CERTA-2010-AVI-527 : Vulnérabilité dans les copieurs Xerox
- CERTA-2010-AVI-528 : Vulnérabilité dans SonicWALL SSL-VPN
- CERTA-2010-AVI-529 : Vulnérabilité dans IBM Tivoli Directory Proxy Server
- CERTA-2010-AVI-530 : Multiples vulnérabilités dans Linux PAM
- CERTA-2010-AVI-531 : Vulnérabilités dans ProFTPD
- CERTA-2010-AVI-532 : Vulnérabilité dans ISC DHCP
- CERTA-2010-AVI-533 : Multiples vulnérabilités dans Bugzilla

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

- CERTA-2010-AVI-499-001 : Multiples vulnérabilités dans les produits Oracle (mise à jour des CVE)

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 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.

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 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.

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_rubrique67.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.

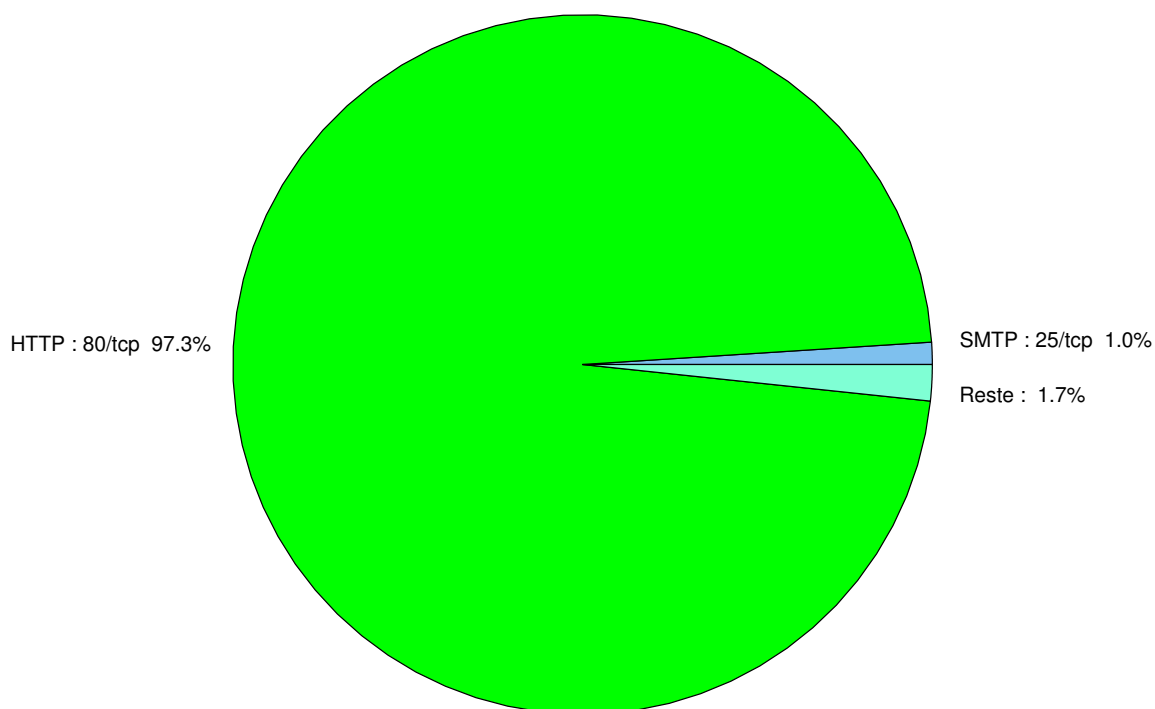


FIG. 1: Répartition relative des ports pour la semaine du 29 octobre au 04 novembre 2010

port	pourcentage
80/tcp	97.36
25/tcp	1.01
1080/tcp	0.45
445/tcp	0.31
1433/tcp	0.2
22/tcp	0.19
2967/tcp	0.14
23/tcp	0.11
3389/tcp	0.08
135/tcp	0.06
3128/tcp	0.03
21/tcp	0.02

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

05 novembre 2010 version initiale.