

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-46

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-046>

Gestion du document

Référence	CERTA-2010-ACT-046
Titre	Bulletin d'actualité 2010-46
Date de la première version	19 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-046.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-046/>

1 Alertes de la semaine

1.1 Logiciels Adobe

Cette semaine, le CERTA a émis l'avis CERTA-2010-AVI-551 relatant la publication, par l'éditeur Adobe, de correctifs permettant de remédier à la vulnérabilité mentionnée dans les alertes CERTA-2010-ALE-018 et CERTA-2010-ALE-020.

La vulnérabilité réside dans le traitement des objets *Flash*. Elle a d'abord été identifiée et corrigée dans les lecteurs Adobe Flash Player.

Des exploitations malveillantes constatées utilisaient des objets au format *Flash* dans des documents au format *PDF*. Les versions 8 d'Adobe Reader et d'Acrobat, un temps suspectées, ne sont pas vulnérables contrairement aux versions 9.

L'éditeur a donc entrepris de mettre à jour les versions 9 de ses lecteurs PDF avec les échéances suivantes :

- le 16 novembre 2010 pour les versions 9 sur Windows et MacOS ;
- le 30 novembre 2010 pour les versions Unix (au sens très large).

Le CERTA recommande d'appliquer ces correctifs dans les plus brefs délais.

1.2 Documentation

- Bulletin de sécurité Adobe apsb10-28 du 16 novembre 2010 :
<http://www.adobe.com/support/security/bulletins/apsb10-28.html>
- Document du CERTA CERTA-2010-AVI-551 du 17 novembre 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-551/index.html>
- Document du CERTA CERTA-2010-ALE-018 du 18 novembre 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-018/index.html>
- Document du CERTA CERTA-2010-ALE-020 du 17 novembre 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-020/index.html>
- Référence CVE CVE-2010-3654 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3654>

2 Mise à jour d'EMET en version 2.0.0.3

EMET (Enhanced Mitigation Experience Toolkit) vient d'être mis à jour en version 2.0.0.3.

Cette mise à jour intervient suite à des problèmes de compatibilité avec les mécanismes de mise à jour de certains produits comme Adobe Reader et Acrobat ou Google Chrome. Dans certaines configurations, EMET pouvait bloquer les mises à jour ou rendre nécessaire un redémarrage.

Une description détaillée du problème se trouve sur le site *Technet* (cf. la section Documentation).

Documentation

- Entrée de blog Technet du 17 novembre 2010 :
<http://blogs.technet.com/b/srd/archive/2010/11/17/emet-update-2-0-0-3-released.aspx>
- Bulletin d'actualité CERTA-2010-ACT-044 du 05 novembre 2010 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-044/index.html>

3 Fausse mise à jour Intel

Après les traditionnelles fausses mises à jour concernant des produits usuels (comme le système d'exploitation Microsoft Windows ou les logiciels de l'éditeur Adobe), c'est au tour du fabricant Intel d'apparaître dans de tels messages.

Un message circule ainsi, faisant croire à des ralentissements, voire des plantages, dus aux pilotes Intel de carte graphique. Un lien vers le site légitime du support du fabricant est donné, suivi d'un minilien supposé diriger vers le téléchargement direct des nouveaux pilotes. Bien entendu, c'est un code malveillant qui est téléchargé lorsque l'on suit ce minilien.

Un minilien est une adresse réticulaire réduite fournie par un tiers. Il permet une redirection avec une adresse de son choix et la diminution de la taille du lien hypertexte associé.

Le recours aux miniliens est subtil : tant que l'utilisateur ne clique pas dessus, il ne sait pas vers quel site il sera dirigé. La méfiance doit donc être de rigueur avant de les suivre, et une vérification préalable de leur légitimité est utile (en demandant par exemple à son RSSI ou à son CERT de rattachement).

Documentation

- Note d'information du CERTA sur l'acquisition de correctifs :
<http://www.certa.ssi.gouv.fr/site/CERTA-2001-INF-004/>

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 au 18 novembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-548 : Multiples vulnérabilités dans Mac OS X
- CERTA-2010-AVI-549 : Vulnérabilité dans libxml2
- CERTA-2010-AVI-551 : Vulnérabilités dans Adobe Reader et Acrobat
- CERTA-2010-AVI-552 : Vulnérabilité dans les imprimantes HP LaserJet
- CERTA-2010-AVI-553 : Multiples vulnérabilités dans VMware ESX et ESXi
- CERTA-2010-AVI-554 : Vulnérabilité dans LANDesk Management Gateway
- CERTA-2010-AVI-555 : Vulnérabilité dans OpenSSL

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

- CERTA-2010-AVI-550-001 : Vulnérabilités dans IBM HTTP Server et WebSphere (ajout des serveurs HTTP hors WebSphere)

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_rubrique67.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.

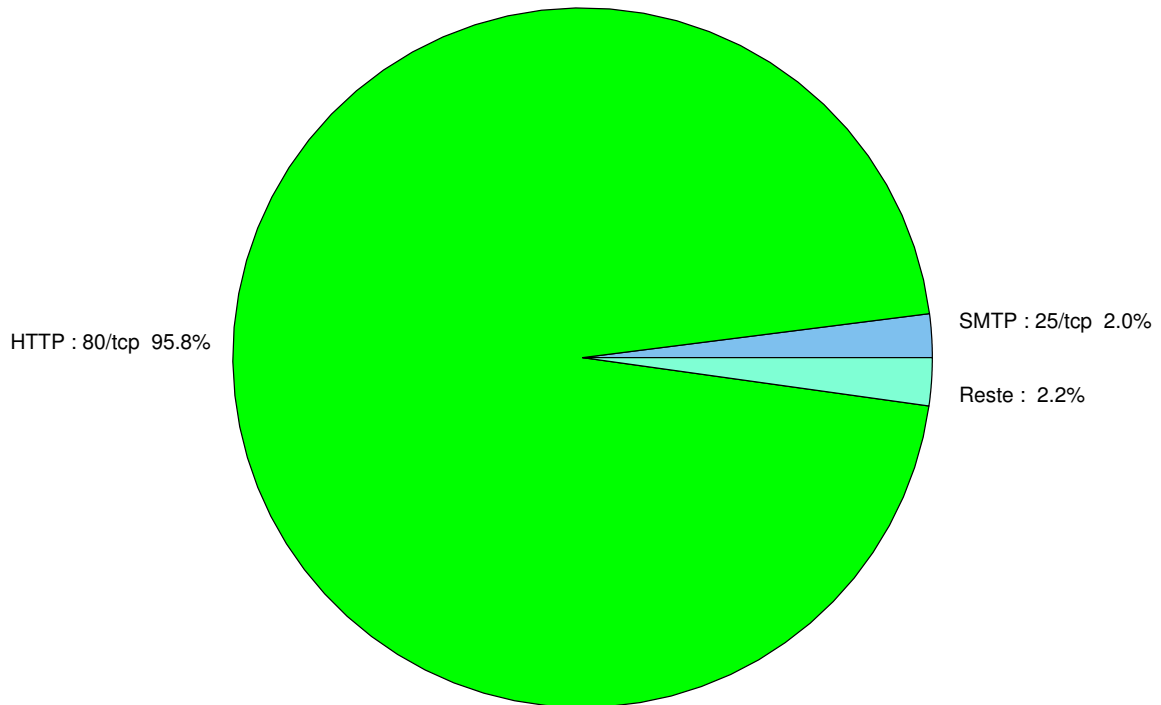


FIG. 1: Répartition relative des ports pour la semaine du 12 au 18 novembre 2010

port	pourcentage
80/tcp	95.92
25/tcp	2
1433/tcp	0.48
1080/tcp	0.43
445/tcp	0.39
23/tcp	0.2
21/tcp	0.14
135/tcp	0.1
3389/tcp	0.09
1434/udp	0.05
3306/tcp	0.02
4899/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

19 novembre 2010 version initiale.