Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 décembre 2010
N° CERTA-2010-ACT-051

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2010-51

Gestion du document

Référence	CERTA-2010-ACT-051
Titre	Bulletin d'actualité 2010-51
Date de la première version	24 décembre 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-051.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-051/

1 Des vœux pas si sincères

Durant cette période de fêtes, accompagnée des traditionels échanges de vœux, le CERTA vous conseille fortement de rester vigilant car il est tentant pour des personnes malveillantes d'exploiter cette tradition. En effet, ceux-ci profitent de l'enthousiasme de cette saison festive pour, entre autre, récolter des données personnelles *via* des sites d'hameçonnage, mettre en place des arnaques, ou encore diffuser des codes malveillants.

Depuis la rentrée 2010, de nombreuses vulnérabilités ont été détectées dans les navigateurs Web, les logiciels de messagerie, les lecteurs de fichiers PDF ou de contenu multimédia tels que *Adobe Flash* qu'il est possible d'intégrer dans une carte de vœux au format électronique. Une partie de ces vulnérabilités permettent l'exécution de code arbitraire à distance.

Le CERTA vous recommande également de refréner l'envie d'installer sur vos postes et ordiphones des thèmes et animations de source douteuse, qui sont autant de portes d'entrées pour des logiciels malveillants.

Documentation

– Note de recommandations CERTA CERTA-2000-REC-002 au sujet des messages de vœux :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-002/

– Note d'information CERTA CERTA-2000-INF-002 relative à la messagerie :
http://www.certa.ssi.gouv.fr/site/CERTA-2000-INF-002/

2 Vulnérabilités de la semaine

2.1 OpenSC

OpenSC est un ensemble de librairies et d'utilitaires permettant d'interagir avec une carte à puce. Il cible plus particulièrement celles supportant des opérations cryptographiques pour les intégrer dans des systèmes d'authentification, de chiffrement et de signature.

Une vulnérabilié dans OpenSC a fait l'objet cette semaine d'un avis sur le site du CERTA.

En effet, un débordement de tampon dans la lecture du numéro de série de certaines cartes à puce permettait à un attaquant ayant accès au système, avec une carte spécialement conçue, d'exécuter du code sur la machine vulnérable.

2.1.1 Impact

Sur les systèmes de type UNIX, OpenSC est utilisé, entre autre, pour gérer l'authentification par carte à puce en utilisant le module PAM-PKCS#11. L'impact est donc important pour ces systèmes si OpenSC est utilisé pour gérer des opérations cryptographiques à partir d'une carte à puce.

OpenSC est également prévu pour être utilisé sur des systèmes fonctionnant sous *Microsoft Windows*. Cependant, la plupart des constructeurs fournissent alors leurs propres bibliothèques. L'impact semble donc être limité sur ces systèmes mais ne doit cependant pas être exclu.

Le CERTA recommande l'application de la mise à jour sur tout système ou logiciel utilisant (directement ou indirectement) la bibliothèque OpenSC.

Documentation

– Avis du CERTA CERTA-2010-AVI-630 du 23 décembre 2010 :
http://www.certa.ssi.gouv.fr/site/CERTA-2010-AVI-630/index.html
– Révision 4913 dans l'arborescence de développement OpenSC :
http://www.opensc-project.org/opensc/changeset/4913

2.2 Service FTP dans IIS

Un code d'exploitation d'une vulnérabilité de la version 7.5 du serveur IIS de Microsoft, livré avec *Windows 7* et *Windows Server 2008 R2*, a donné lieu à quelques discussions.

2.2.1 Plateformes vulnérables

Les plateformes vulnérables sont celles sur lesquelles :
– le serveur IIS s'exécute ;
– le service FTP d'IIS a été installé, ce qui n'est pas la configuration standard ;
– ce service a été activé, ce qui n'est pas automatique lors de l'installation.

Ces conditions rendent peu probable la présence « involontaire » d'un service FTP d'IIS actif. En cas de doute, la commande en ligne *service control* (SC) permet connaitre l'état du service FTP d'IIS :

```
prompt>sc query ftpsvc
```

2.2.2 Impact

L'impact est encore incertain. En l'état actuel des recherches, le code d'exploitation ne provoque qu'un arrêt inopiné du service FTP. Le reste du serveur IIS n'est pas touché, en particulier les services HTTP et HTTPS.

S'il a été fait mention d'exécution de code arbitraire à distance, l'auteur de la preuve de faisabilité ne le prétend pas et l'éditeur ne l'atteste pas.

Le CERTA reste attentif à l'évolution de la situation et tiendra sa communauté informée.

2.2.3 Recommandations

En tout état de cause et sous réserve du respect de la PSSI, le CERTA recommande :
- de désactiver, voire de désinstaller le service FTP d'IIS si celui-ci n'est pas utilisé ;
- de restreindre l'accès aux seuls utilisateurs autorisés et de mettre en place les mesures de filtrage adaptées ;
- de journaliser les évènements, les accès et les tentatives, sur le serveur et sur les dispositifs de filtrage ;
- d'analyser les journaux ainsi produits, si possible au fil de l'eau, pour détecter au plus vite des attaques.

2.2.4 Documentation

- Bloc-notes Microsoft SRD, billet du 22 décembre 2010 :
  http://blogs.technet.com/b/srd/archive/2010/12/22/assessing-an-iis-ftp-7-5-unauthenticated-denial-of-service-vulnerability.aspx
- Manuel de la commande SC
  http://technet.microsoft.com/en-us/library/bb490995.aspx
- Référence CVE CVE-2010-3972 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3972

2.3 Microsoft Internet Explorer

Microsoft Internet Explorer a fait l'objet d'une alerte cette semaine. Toutes les versions (6, 7 et 8) du navigateur sont vulnérables et permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance au moyen d'une page web spécialement conçue.

Une preuve de faisabilité est désormais disponible sur l'Internet. Elle exploite une vulnérabilité dans les feuilles de styles CSS due à une utilisation de mémoire libérée.

L'ASLR (*Address Space Layout Randomization*) et le DEP (*Data Execution Prevention*) ont été contournés. Cependant l'utilisation d'EMET (*Enhanced Mitigation Experience Toolkit*) et la désactivation du Javascript permettent de limiter la possibilité d'exploitation de la vulnérabilité.

Dans l'attente d'un correctif de la part de l'éditeur, le CERTA recommande de ne naviguer que sur des sites de confiance ou d'utiliser un navigateur alternatif.

Documentation

- Alerte CERTA CERTA-2010-ALE-021 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-021/index.html
- Bulletin de sécurité Microsoft 2488013 du 22 décembre 2010 :
  http://www.microsoft.com/technet/security/advisory/2488013.mspx
- Bloc-notes Microsoft SRD, billet du 22 décembre 2010 :
  http://blogs.technet.com/b/srd/archive/2010/12/22/new-internet-explorer-vulnerability-affecting-all-versions-of-ie.aspx
- Référence CVE CVE-2010-3971 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3971

3 Rappel des avis émis

Dans la période du 17 au 24 décembre 2010, le CERTA a émis les avis suivants :

- CERTA-2010-AVI-614 : Multiples vulnérabilités dans TYPO3
- CERTA-2010-AVI-615 : Multiples vulnérabilités dans Opera
- CERTA-2010-AVI-616 : Vulnérabilité dans phpMyFAQ
- CERTA-2010-AVI-617 : Vulnérabilité dans Symantec Endpoint Protection
- CERTA-2010-AVI-618 : Vulnérabilités dans PHP
- CERTA-2010-AVI-619 : Vulnérabilité dans le noyau Linux
- CERTA-2010-AVI-620 : Vulnérabilités dans AirPort Extreme Base Station et Time Capsule
- CERTA-2010-AVI-621 : Vulnérabilités dans IBM Tivoli Storage Manager

– CERTA-2010-AVI-622 : Vulnérabilités dans IBM Rational ClearQuest
– CERTA-2010-AVI-623 : Vulnérabilité dans ISC DHCP
– CERTA-2010-AVI-624 : Vulnérabilités dans MyBB
– CERTA-2010-AVI-625 : Vulnérabilité de produits Kerio
– CERTA-2010-AVI-626 : Vulnérabilité dans VMware ESXi
– CERTA-2010-AVI-627 : Vulnérabilités dans Blue Coat Reporter
– CERTA-2010-AVI-628 : Vulnérabilité dans HP Power Manager
– CERTA-2010-AVI-629 : Vulnérabilité dans HP StorageWorks Storage Mirroring
– CERTA-2010-AVI-630 : Vulnérabilité dans OpenSC

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

– CERTA-2010-AVI-575-001 : Vulnérabilités dans BIND (ajout de la référence au bulletin de sécurité Red Hat)

4 Actions suggérées

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 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

5 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.

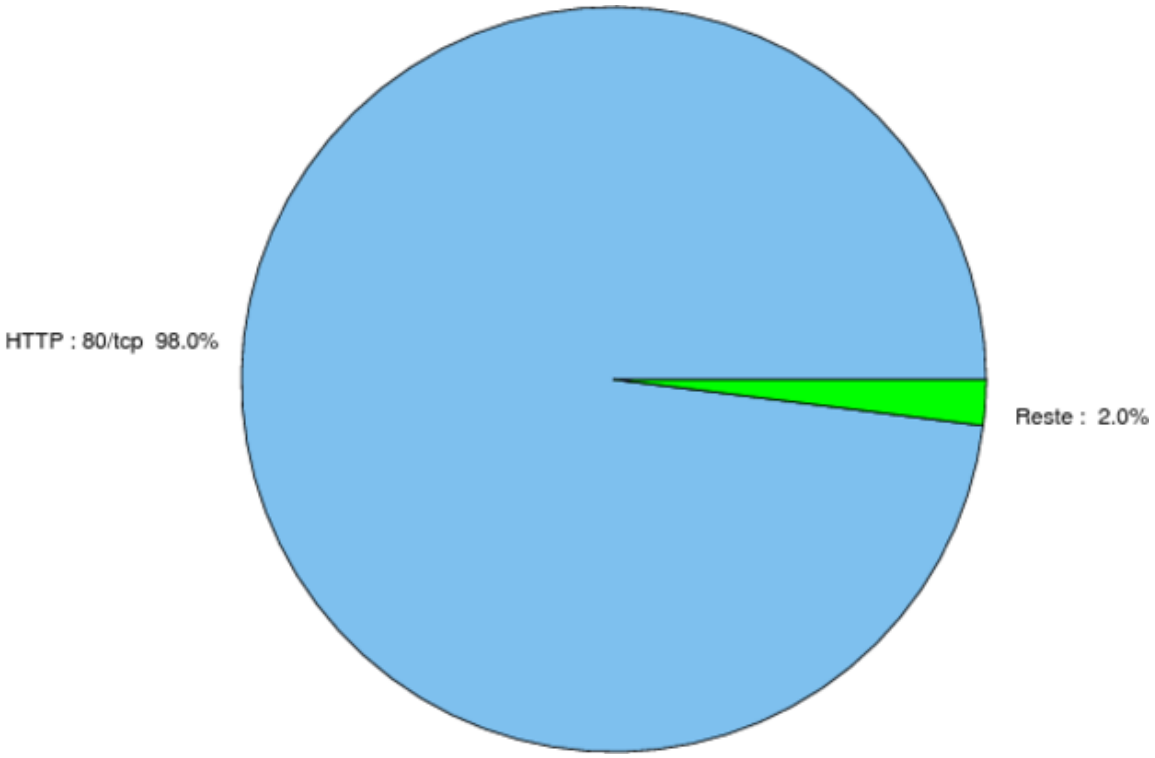

FIG. 1: Répartition relative des ports pour la semaine du 10 au 16 décembre 2010

port	pourcentage
80/tcp	98.28
25/tcp	0.84
1080/tcp	0.19
1433/tcp	0.17
23/tcp	0.14
22/tcp	0.12
3389/tcp	0.08
135/tcp	0.04
3127/tcp	0.03
3128/tcp	0.02
3306/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

1 Gestion du document 1
2 Paquets rejetés 6

Gestion détaillée du document

24 décembre 2010 version initiale.