Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 janvier 2011
N° CERTA-2011-ACT-004

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-04

Gestion du document

Référence	CERTA-2011-ACT-004
Titre	Bulletin d'actualité 2011-04
Date de la première version	28 janvier 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-004.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-004/

1 Incidents de la semaine

1.1 FCKeditor, le retour

Le logiciel FCKeditor, désormais appelé CKEditor, est un éditeur de texte qui peut être utilisé pour des pages Web. Il est doté d'une fonctionnalité de dépôt de fichiers. Cette fonctionnalité peut aisément être détournée par un attaquant pour charger sur le serveur de fichiers, de la simple défiguration à l'entreposage de contenus illégaux. Il est directement intégré dans certains gestionnaires de contenu. Ainsi, des contributions au projet SPIP permettent l'intégration de ce logiciel.

Le CERTA a signalé à l'un de ses correspondants une insertion illégitime de fichier sur l'un de ses sites web. L'analyse a rapidement montré l'utilisation du logiciel FCKeditor par l'intrus pour déposer son fichier. Le CERTA avait fait part d'une vague d'intrusions basées sur cet utilitaire (voir section Documentation). L'incident de cette semaine prouve que la méthode a toujours cours.

Dans le même temps, plusieurs défigurations touchant des sites du secteur privé ont été perpétrées par le même intrus. Certains de ces sites utilisent le même gestionnaire de contenu que le correspondant du CERTA cité ci-dessus. Il n'est pas exclus que l'éditeur intégré a été également utilisé.

1.1.1 Recommandations

Le CERTA recommande, face à cette situation :

- de mettre, comme toujours, ses systèmes et ses logiciels à jour ;
- de n'autoriser l'accès aux moyens de modifier le contenu (FCKeditor, FTP, SSH...) qu'aux utilisateurs et aux adresses nécessaires ;
- d'utiliser des mots de passe forts pour ces modifications ;
- de (faire) vérifier régulièrement la salubrité des postes de travail à partir desquels les modifications sont faites. Un mot de passe fort est en effet inutile si un cheval de Troie sur un tel poste copie et diffuse à volonté ce mot de passe ;
- de n'allouer que les droits indispensables aux processus liés à ces outils de modification ;
- de désactiver ces moyens dès lors qu'ils ne sont plus indispensables ;
- de mettre en place un système de vérification de l'intégrité du serveur ;
- de journaliser les modifications et d'analyser régulièrement les journaux.

La vigilance doit être encore plus grande lorsque le site web est sur un serveur mutualisé. Le défaut de cloisonnement ou des droits trop importants peuvent permettre à un intrus d'entrer par un site faible (par exemple avec FCKeditor accessible à tout l'Internet) pour rebondir ensuite sur tous les sites web hébergés.

1.1.2 Documentation

- Bulletin d'actualité du CERTA CERTA-2010-ACT-044 du 05 novembre 2010 : http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-044/index.html
- « Les mots de passe » CERTA-2005-INF-001 du 12 avril 2007 : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-001
- « Bonnes pratiques concernant l'hébergement mutualisé » CERTA-2005-INF-005 du 19 décembre 2005 : http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005

2 Rappel des avis émis

Dans la période du 21 au 27 janvier 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-027 : Vulnérabilité dans IBM WebSphere
- CERTA-2011-AVI-028 : Vulnérabilité dans IBM Tivoli
- CERTA-2011-AVI-029 : Vulnérabilité dans HP OpenView Storage Data Protector
- CERTA-2011-AVI-030 : Vulnérabilité dans Cisco Linksys WRT54GC
- CERTA-2011-AVI-031 : Multiples vulnérabilités dans Bugzilla
- CERTA-2011-AVI-032 : Vulnérabilités dans syslog-ng
- CERTA-2011-AVI-033 : Multiples vulnérabilités dans Cisco Content Service Gateway
- CERTA-2011-AVI-034 : Vulnérabilité dans HP OpenView Storage Data Protector
- CERTA-2011-AVI-035 : Vulnérabilité dans HP BAC et BSM
- CERTA-2011-AVI-036 : Multiples vulnérabilités dans les produits Symantec
- CERTA-2011-AVI-037 : Vulnérabilités dans Opera
- CERTA-2011-AVI-038 : Vulnérabilité dans Novell GroupWise Internet Agent

3 Actions suggérées

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

3.6 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.

3.7 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

4 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.

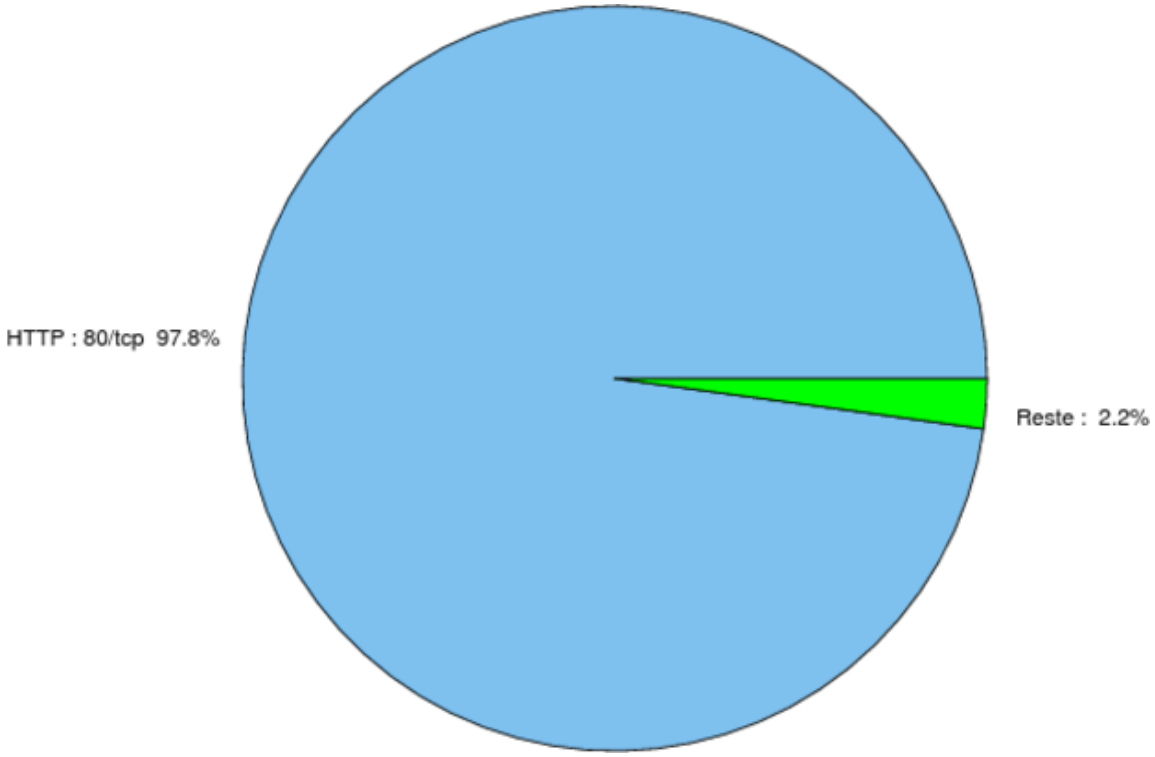

FIG. 1: Répartition relative des ports pour la semaine du 21 au 27 janvier 2011

port	pourcentage
80/tcp	97.93
25/tcp	0.77
1433/tcp	0.49
445/tcp	0.15
1080/tcp	0.14
22/tcp	0.11
3389/tcp	0.08
2967/tcp	0.03
1434/udp	0.02
4899/tcp	0.01

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

28 janvier 2011 version initiale.