Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 septembre 2011
N° CERTA-2011-ACT-038

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-38

Gestion du document

Référence	CERTA-2011-ACT-038
Titre	Bulletin d'actualité 2011-38
Date de la première version	23 septembre 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-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-2011-ACT-038/

1 Incidents de la semaine

CKEditor, FCKEditor : une porte d'entrée pour les intrus

CKEditor, comme son prédécesseur *FCKEditor*, est un éditeur texte et HTML WYSIWYG distribué sous plusieurs licences de logiciels libres.

Il permet d'enrichir le site Web sur lequel il est présent, par la création en ligne de pages, de commentaires ou de billets. Il est intégré ou utilisable sous forme de module dans des gestionnaires de contenu (CMS) ou dans des développements spécifiques.

1.1 Incidents récents

Deux incidents très récents ayant affecté la communauté des utilisateurs du CERTA ont un point commun : *FCKEditor* a servi de porte d'entrée aux intrus.

Dans un cas, le chargement d'un fichier a permis à l'attaquant l'escalade de permissions jusqu'à devenir super utilisateur. Il a alors compromis tous les sites Web présents sur le serveur physique.

Dans un autre cas, la compromission du site Web a permis des rebonds sur d'autres serveurs du réseau.

1.2 Recommandations

Des précautions élémentaires ont déjà été recommandées par le CERTA pour limiter l'accès de cet éditeur aux utilisateurs légitimes et pour limiter l'impact d'un détournement de son utilisation (voir la sous-section Documentation).

Il est donc indispensable de rappeler quelques règles :

- faire l'inventaire des moyens de modifier le contenu du serveur Web et du serveur sous-jacent (*FCKEditor*, WebDAV, FTP, SSH...). Ces moyens peuvent être peu visibles car intégrés à des logiciels applicatifs (CMS, par exemple) ;
- mettre, comme toujours, ses systèmes et ses logiciels à jour ;
- n'autoriser l'accès aux moyens de modifier le contenu qu'aux utilisateurs et aux adresses nécessaires. Ceci implique un filtrage réseau et une authentification adaptée des utilisateurs ;
- utiliser des mots de passe forts pour ces moyens de modification et, si le contexte l'exige, une authentification forte du client ;
- (faire) vérifier régulièrement l'intégrité 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 ;
- n'allouer que les droits indispensables aux processus liés à ces outils de modification ;
- désactiver ces moyens dès lors qu'ils ne sont plus indispensables ;
- mettre en place un système de vérification de l'intégrité du serveur ;
- journaliser les modifications et analyser régulièrement les journaux.

La vigilance doit être encore plus grande lorsque le site Web est sur un serveur mutualisé.

1.3 Documentation

- Document du CERTA CERTA-2011-ACT-004 du 28 janvier 2011 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2011-ACT-004/
- Document du CERTA CERTA-2010-ACT-044 du 05 novembre 2010 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-044/

2 Élévation de privilèges d'administrateur local à administrateur de domaine

Lors des investigations menées par le CERTA, nous sommes amenés à constater des compromissions profondes d'environnements de production. Fréquemment ces situations sont dues à la méconnaissance des mécanismes permettant à un attaquant d'élever des privilèges d'administrateur local d'un poste ou serveur compromis vers des privilèges d'administration de la globalité du système d'information.

Ces attaques, de la plus simple à la plus sophistiquée, de la plus rapide à la plus lente sont régulièrement constatées dans les environnements sur lesquels le CERTA est intervenu.

Notre bulletin d'actualité se propose de détailler certaines de ces attaques ainsi que les mesures permettant de limiter l'exposition aux risques et aux impacts dans vos environnements. Pour commencer, le bulletin d'actualité se concentrera sur les environnements Microsoft Windows. L'administrateur d'une machine Windows (légitime ou illégitime) dispose des privilèges nécessaires pour inspecter, modifier ou « trahir » le système d'exploitation et les applications de cette machine. Tout ce que le système recèle de mots de passe, de clés, de condensés ou plus généralement de « secret » est accessible à un code disposant des privilèges d'administration locaux.

Force est de constater que l'attaquant dispose aussi d'un autre levier dans son attaque : le temps. Nous remarquons qu'un attaquant peut patienter des semaines voire des mois afin qu'un évènement rare ou improbable se produise et lui apporte les clés du système d'information. Pour illustrer ce propos, nous allons aborder les premières techniques simples (et redoutables) fréquemment exploitées.

Très Simple : l'implantation de clés de registre

Attaque :

Sous Microsoft Windows, un attaquant ayant les privilèges d'administration sur un poste dispose des droits d'écriture dans la ruche HKEY_LOCAL_MACHINE. Il peut alors y inscrire le lancement automatique d'une commande de son choix à chaque ouverture de session, que le logiciel soit ou non malveillant. L'attaquant n'a

alors plus qu'à attendre l'ouverture d'une session avec un compte « puissant » pour disposer de ses droits et privilèges. Par exemple, le ver Conficker a compromis un nombre bien plus grand de systèmes en utilisant cette technique qu'en exploitant la vulnérabilité adressée par le correctif MS08-067.

Prévention :

Il n'existe pas de défense absolue contre cette attaque. Néanmoins les mesures habituelles de défense en profondeur pourront très largement en diminuer la probabilité et l'impact :

- ne pas ouvrir de session interactive avec un compte d'administration « puissant » sur des postes d'utilisateurs. Au contraire, utiliser RunAs ou « exécuter en tant que » pour élever les privilèges des seuls processus nécessaires.
- ne pas utiliser de compte d'administration du domaine pour intervenir sur des postes utilisateur potentiellement compromis (recommandation typiquement destinée aux équipes de support).

Simple et rapide : l'énumération des sessions de la machine compromise

Attaque :

Lors de la compromission d'une machine, l'attaquant disposant des droits locaux d'administration locale peut énumérer les processus présents sur un poste et « emprunter » les droits associés à ces processus. Si un processus s'exécute sur un poste compromis en utilisant un compte puissant du domaine, alors l'attaquant peut s'associer à sa session et usurper ses privilèges.

Prévention :

Il convient de s'assurer que des processus ne s'exécutent pas avec des comptes puissants du domaine. Ainsi les scripts, les services, les tâches planifiées ne sont exécutés qu'au moyen de comptes restreints aux seuls privilèges requis par cette tâche.

À suivre…

3 Rappel des avis émis

Dans la période du 16 au 22 septembre 2011, le CERTA a émis les publications suivantes :

- CERTA-2011-AVI-521 : Vulnérabilité dans JBoss
- CERTA-2011-AVI-522 : Vulnérabilités dans phpMyAdmin
- CERTA-2011-AVI-523 : Vulnérabilité dans HP Network Manager i
- CERTA-2011-AVI-524 : Multiples vulnérabilités dans Blue Coat Director
- CERTA-2011-AVI-525 : Vulnérabilités dans Red Hat Network Satellite
- CERTA-2011-AVI-526 : Vulnérabilité dans EMC Ionix
- CERTA-2011-AVI-527 : Vulnérabilités dans IBM WebSphere Commerce Enterprise
- CERTA-2011-AVI-528 : Vulnérabilités dans Google Chrome
- CERTA-2011-AVI-529 : Vulnérabilité dans Cisco Identity Services Engine
- CERTA-2011-AVI-530 : Vulnérabilité dans les produits Oracle
- CERTA-2011-AVI-531 : Multiple vulnérabilités dans Adobe Flash Player

Durant la même période, les publications suivantes ont été mises à jour :

- CERTA-2011-AVI-488-001 : Vulnérabilité dans les produits Cisco (modification du titre et ajout de systèmes vulnérables)
- CERTA-2011-AVI-503-001 : Multiples vulnérabilités dans Wireshark (ajout de références CVE)
- CERTA-2011-AVI-505-001 : Vulnérabilités dans Cyrus IMAPd (ajout d'une deuxième vulnérabilité et de précisions sur la première)

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_rubrique62.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.

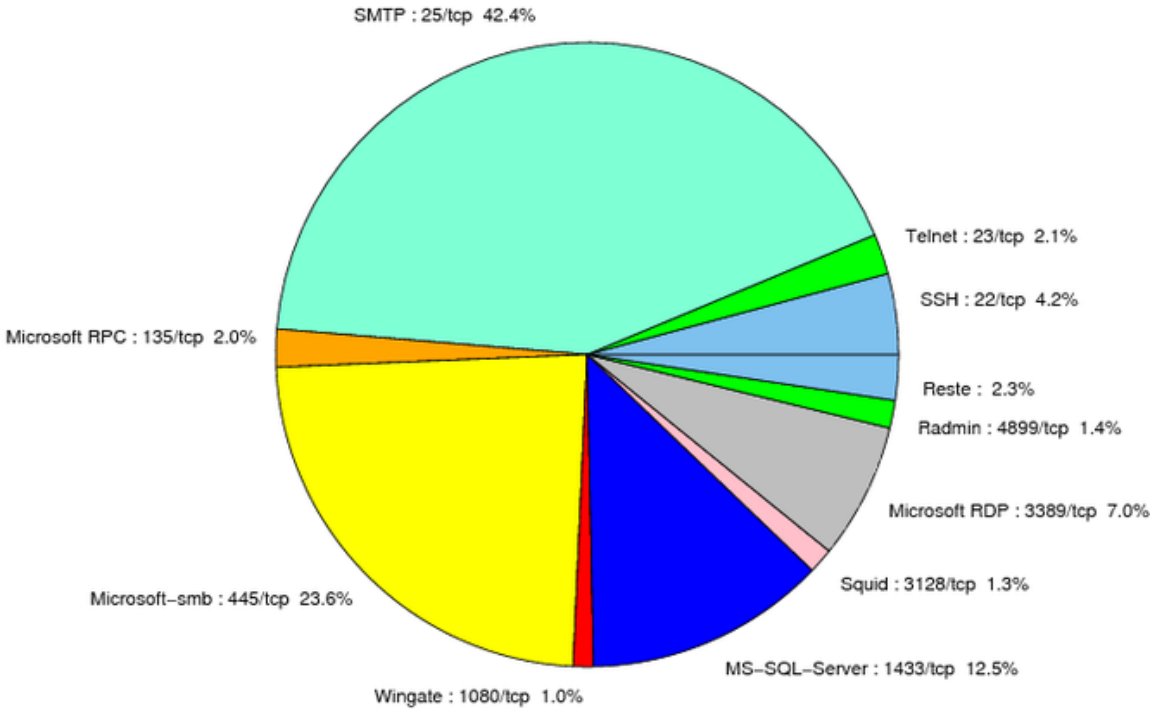

FIG. 1: Répartition relative des ports pour la semaine du 16 au 22 septembre 2011

port	pourcentage
25/tcp	42.42
445/tcp	23.62
1433/tcp	12.53
80/tcp	7.57
3389/tcp	7.04
22/tcp	4.17
23/tcp	2.08
135/tcp	1.95
4899/tcp	1.43
3128/tcp	1.3
1080/tcp	1.04
2967/tcp	0.65
3306/tcp	0.52

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

23 septembre 2011 version initiale.