Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 mars 2011
N° CERTA-2011-ACT-012

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-12

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-2011-ACT-012`

Gestion du document

Référence	CERTA-2011-ACT-012
Titre	Bulletin d'actualité 2011-12
Date de la première version	25 mars 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-012.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-012/

1 CDN et protection contre les DDOS

Il est souvent d'usage de dire que les CDN pour `Content Delivery Network` permettent de se prémunir des attaques par déni de service distribué.

Le concept de CDN est relativement simple, il consiste, pour un site donné, en la mise en cache de son contenu sur de nombreuses machines (le CDN à proprement parlé). L'usage particulier des DNS permettra d'aiguiller un client vers le cache le plus proche en terme de temps et de nombre de sauts. Si le cache consulté dispose déjà de la page, c'est lui qui distribue le contenu sinon il s'adresse d'abord au serveur source (« le vrai serveur ») afin d'obtenir la page et la délivre ensuite au client.

L'idée est évidemment de supporter une charge plus importante en distribuant largement le contenu au sein du CDN qui pourra le fournir efficacement et localement au client.

Cependant, il y a quelque temps, des chercheurs ont montré qu'il pouvait y avoir un biais dans ce système. En effet, comme tout système de cache, le CDN fonctionne bien dans le cas de contenus statiques comme des pages en HTML simple, des images ou vidéos. Si le site source est dynamique, cela se complique...

En effet, pour chaque requête spécifique, un nouvelle mise en cache aura lieu. Ainsi, si l'on prend une requête *GET* avec quelques paramètres, il suffit que l'un de ces paramètres varie pour qu'une nouvelle mise en cache ait

lieu suivant la règle *« une requête = un contenu spécifique »*. Une nouvelle requête au serveur source sera alors engendrée. Dans ce cas précis, le CDN n'est plus d'une grande utilité puisque pour chaque requête de client, on a une requête sur le serveur source.

Un *botnet* utilisant ce genre de technique serait à même d'annuler en partie les effets bénéfiques de l'utilisation d'un CDN. Cependant, il est alors possible d'identifier la présence de ces machines zombies dans un réseau car elle vont occasionner un important trafic à destination de la cible avec des requêtes variant très peu mais toujours sur la même page.

Ces même chercheurs ont d'ailleurs montré qu'il était possible d'améliorer la technique d'attaque pour que ce défaut particulier du *botnet* soit supprimé et que l'attaque en DDOS exploite à son avantage et de façon optimale la présence du CDN.

2 Correction de l'alerte CERTA-2011-ALE-002 : produits Adobe

Comme prévu par Adobe, la vulnérabilité annoncée la semaine dernière (voir l'alerte CERTA-2011-ALE-002) concernant les logiciels Adobe Flash Player, Adobe Reader et Adobe Acrobat a été corrigée pour ces produits. Pour rappel, cette vulnérabilité permet l'exécution de code arbitraire à distance via des documents spécialement conçus.

Compte tenu du fait que cette vulnérabilité est actuellement exploitée activement sur l'Internet, le CERTA recommande vivement l'installation de ces mises à jour.

Documentation

- Bulletin de sécurité Adobe Flash apsb11-05 du 21 mars 2011 :
  http://www.adobe.com/support/security/bulletins/apsb11-05.html
- Bulletin de sécurité Adobe Reader et Acrobat apsb11-06 du 21 mars 2011 :
  http://www.adobe.com/support/security/bulletins/apsb11-06.html
- Bulletin de sécurité Adobe apsa11-01 du 14 mars 2011 :
  http://www.adobe.com/support/security/advisories/apsa11-01.html
- Référence CVE CVE-2011-0609 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0609
- Correctif Google Chrome :
  http://www.google.com/support/chrome/bin/answer.py?hl=en?answer=95414

3 Vrais faux certificats SSL

Le CERTA a émis un avis (CERTA-2011-AVI-169) à propos de l'émission, et de la révocation par certains navigateurs, de certificats SSL. Un compte d'une autorité d'enregistrement (RA) affiliée à l'autorité de certification (CA) Comodo présentait une vulnérabilité. Cette brèche a été exploitée par des attaquants qui ont émis frauduleusement neuf certificats sur sept domaines différents. L'un de ces faux certificats a été utilisé pour monter une attaque trompant les internautes.

L'incident a été detecté le 15 mars 2011. L'autorité de certification immédiatement révoqué ces certificats. Elle a également contacté des éditeurs de logiciels pour la mise en liste noire de ces certificats. La mise à jour des listes de révocation (CRL) et des serveurs de vérification OCSP ne suffit pas à se prémunir contre l'utilisation de ces certificats :

- l'utilisateur d'un navigateur peut avoir désactivé ces modes de contrôle de validité des certificats ;
- le comportement du navigateur, en l'absence de réponse du serveur OCSP ou du serveur de CRL peut être de considérer que le certificat n'est pas révoqué ;
- l'attaquant qui exploite la fraude précédente en s'interposant entre des internautes et le vrai serveur peut également s'interposer entre le navigateuret le serveur, OCSP ou de CRL.

Les navigateurs suivants ont fait l'objet de mises à jour :

- Chrome ;
- Firefox et Seamonkey ;

– Iceweasel ;
– Internet Explorer.

Au-delà des navigateurs, d'autres logiciels clients peuvent être touchés : messagerie, messagerie instantanée...

4 SCADA - Publications de vulnérabilités

4.1 Actualité

Cette semaine a vu se mutiplier les publications de vulnérabilités des systèmes industriels, ou d'outils les exploitant :

– un chercheur détaille et publie des preuves de faisabilité visant Siemens Technomatix FactoryLink, Iconics GENESIS32 et GENESIS64, 7-Technologies ICSS et Realwin Realflex SCADA. L'impact des ces exploitations va de la divulgation d'informations à l'exécution de code arbitraire à distance. Plusieurs vulnérabilités ne sont pas corrigées ;
– un outil de test d'exploitation de vulnérabilités, récentes ou non, dont une non corrigée, avec la même diversité d'impacts, vise par exemple Moxa DMT, TRACE MODE Data Centre, Ecava IntegraXor et GE Fanuc Real-Time Portal ;
– l'ICS-CERT, *alter ego* de l'US-CERT pour les systèmes industriels, publie six bulletins relatifs aux vulnérabilités de plusieurs de ces produits.

Cette actualité montre que les systèmes industriels deviennent un terrain d'attaques informatiques qui se banalise. Des preuves de faisablité, détournables en code d'exploitataion, sont publiées. Des outils, dits de test, mais utilisables de manière hostile, sont téléchargeables.

La réactivité des éditeurs et des intégrateurs de systèmes industriels sera mise à rude épreuve.

4.2 Recommandations

Face à ces menaces qui se « démocratisent », le CERTA recommande, dans la mesure des possibilités des systèmes et des contraintes règlementaires et industrielles, au moins l'application des mesures classiques d'hygiène informatique :

– inventaire des produits utilisés et des versions en exploitation ;
– suivi des informations des éditeurs sur ces logiciels, dont les vulnérabilités ;
– mise à jour des logiciels ;
– à défaut, mise en place des mesures d'atténuation de la menace ;
– cloisonnement de l'architecture et des flux réseau, filtrage et journalisation associés ;
– surveillance des interconnexions ;
– séparation des rôles, notamment entre administrateur, programmeur de système et exploitant ;
– utilisation des fonctions d'authentification offertes (SCADA, protocoles, automates) ;
– utilisation de mots de passe forts et remplacement des mots de passe usine ;
– sensibilisation de tous les personnels ;
– protection des accès physiques et traçabilité ;
– attention particulière aux opérations de maintenance ;
– politique restrictive vis-à-vis des supports amovibles et désactivation des automatismes qui leur sont liés...

4.3 Documentation

– Site de l'ICS-CERT :
http://www.us-cert.gov/control_systems/

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 18 au 24 mars 2011, le CERTA a émis les avis suivants :

– CERTA-2011-AVI-157 : Vulnérabilité dans EMC RSA Access Manager Server
– CERTA-2011-AVI-158 : Multiples vulnérabilités dans Lotus Quickr
– CERTA-2011-AVI-159 : Vulnérabilités dans SAP NetWeaver
– CERTA-2011-AVI-161 : Vulnérabilité dans ProFTPD
– CERTA-2011-AVI-162 : Multiples vulnérabilités dans Mac OS X
– CERTA-2011-AVI-163 : Vulnérabilité dans Logwatch
– CERTA-2011-AVI-164 : Vulnérabilité dans Xpdf sur Linux
– CERTA-2011-AVI-165 : Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat
– CERTA-2011-AVI-166 : Vulnérabilité dans Symantec LiveUpdate Administrator
– CERTA-2011-AVI-167 : Vulnérabilités dans VLC Media Player
– CERTA-2011-AVI-168 : Vulnérabilités dans Quagga
– CERTA-2011-AVI-169 : Certificats SSL frauduleux

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

– CERTA-2011-AVI-101-001 : Multiples vulnérabilités dans Ruby (ajout des références CVE)
– CERTA-2011-AVI-160-001 : Vulnérabilités dans PHP (ajout de vulnérabilités et 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 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.

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 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.

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_rubrique62.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.

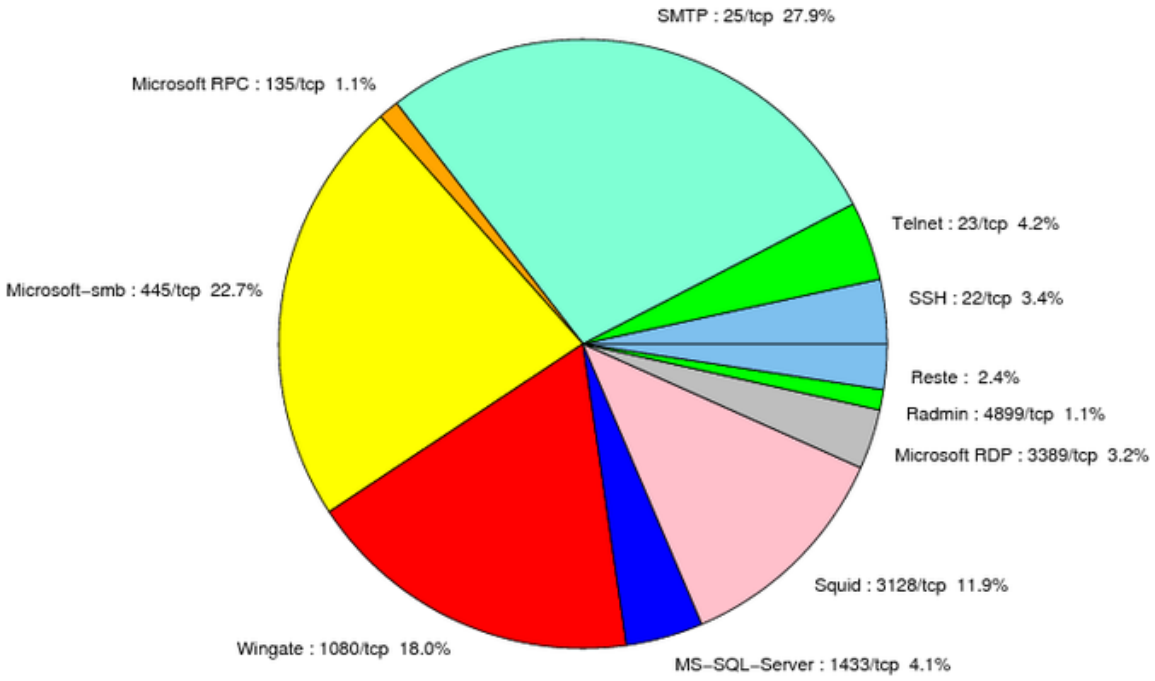

FIG. 1: Répartition relative des ports pour la semaine du 18 au 24 mars 2011

port	pourcentage
25/tcp	27.9
445/tcp	22.71
1080/tcp	17.98
3128/tcp	11.93
23/tcp	4.18
1433/tcp	4.1
80/tcp	3.87
22/tcp	3.41
3389/tcp	3.17
4899/tcp	1.08
2967/tcp	0.93
3306/tcp	0.46
10080/tcp	0.07

TAB. 2: Paquets rejetés

Liste des tableaux

Gestion détaillée du document

25 mars 2011 version initiale.