



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 juin 2011
N° CERTA-2011-ACT-025

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2011-25

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-025>

Gestion du document

Référence	CERTA-2011-ACT-025
Titre	Bulletin d'actualité 2011-25
Date de la première version	24 juin 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.

1 Rappel sur la vulnérabilité Debian OpenSSL de 2008

En 2008, le CERTA publiait dans le bulletin d'actualité CERTA-2008-ACT-020 une vulnérabilité dans le générateur de pseudo-aléa utilisé par le paquet *OpenSSL* distribué par *Debian*. Toutes les clés privées créées par cette version du paquet présentent des faiblesses cryptographiques permettant, entre-autre, à une personne malveillante de réaliser des attaques de type « homme au milieu » (*Man in the middle*). Cette semaine, le CERTA a été alerté de l'utilisation d'un de ces certificats générés avec une clé faible sur un serveur de consultation de courrier IMAPS.

Pour rappel, toute clé privée produite avec la bibliothèque *OpenSSL*, et tout certificat signé avec l'une d'entre-elles sous les systèmes *Debian* et *Ubuntu* entre le 8 avril 2007 et le 15 mai 2008 sont potentiellement vulnérables. Les détails sont disponibles dans les avis CERTA-2008-AVI-246 et CERTA-2008-AVI-248.

Plusieurs outils sont disponibles pour automatiser la vérification des éléments cryptographiques :

- la commande `openssl-vuln` disponible dans le paquet `openssl-blacklist` ;
- la commande `ssh-vulnkey` disponible dans le paquet `openssh-client`.

D'autre part, le projet *Debian* fournit des méthodes pour procéder au recouvrement des clés faibles pour différents paquets victimes de la vulnérabilité *OpenSSL* comme *OpenVPN*, *cryptsetup* ou *OpenSSH*.

Le CERTA recommande d'effectuer la vérification, et au besoin le changement des clés privées et certificats utilisés par des protocoles sécurisés sous systèmes basés sur *Debian* qui ont pu être créés avec la bibliothèque *OpenSSL* vulnérable.

Documentation

- Recouvrement de clés faibles pour plusieurs paquets utilisant des méthodes cryptographiques :
<http://www.debian.org/security/key-rollover/>
- Page du Wiki Debian concernant la vulnérabilité :
<http://wiki.debian.org>
- Avis CERTA-2008-AVI-246 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-246/>
- Avis CERTA-2008-AVI-248 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-248/>

2 Redirections depuis des sites Web compromis

Le CERTA a été amené à traiter récemment le cas de plusieurs sites Web compromis. La compromission de ces sites est caractérisée par la présence de code effectuant une redirection vers d'autres sites, ces derniers hébergeant soit des pages de *phishing* bancaire, soit des offres commerciales pour des produits pharmaceutiques.

La principale particularité de ces incidents vient du fait que la redirection ne survient pas systématiquement. En effet, si l'accès se fait en tapant l'adresse de la page dans le navigateur, aucune redirection n'est constatée, et les pages légitimes sont affichées. Par contre, si la visite se fait en suivant un lien particulier, alors l'internaute est redirigé vers un autre site Web.

Un tel comportement est caractéristique d'une compromission du serveur Web visité initialement. Les redirections sont le fait de scripts PHP ou de fichiers `.htaccess` malveillants. Elles surviennent typiquement lorsque le client de navigation annonce un champ *referer* particulier (par exemple, celui d'un moteur de recherche avec des mots-clefs spécifiques).

La détection des incidents exploitant cette mécanique est difficile. Elle suppose que l'administrateur du site Web compromis accepte de suivre un lien pour constater de lui-même l'intrusion, ce qui peut ne pas être conforme avec la politique de sécurité. Il peut donc être préférable d'accorder davantage de confiance au tiers qui signale le problème, surtout si c'est un CSIRT de référence.

3 Mise à jour Firefox et changement de version

Cette semaine la fondation Mozilla a publié une mise à jour de son navigateur Firefox. Cette mise à jour marque le passage en version 5.0 du logiciel et comble de nombreuses vulnérabilités, détaillées dans l'avis CERTA-2011-AVI-365.

Mozilla a profité de cette nouvelle mouture pour changer sa politique de gestion des versions de Firefox. En effet, la récente version 4 sortie le 22 mars 2011 n'est plus maintenue. Les deux seules branches encore maintenues sont les branches 3.6 et 5. Il est donc fortement recommandé aux utilisateurs de la version 4 de mettre à jour le logiciel en version 5.0.

Mozilla a pris la décision d'augmenter le rythme de publication des versions majeures de son navigateur. Ainsi, le délai entre deux versions majeures devraient se situer entre 16 et 18 semaines.

Documentation

- Avis CERTA-2011-AVI-365 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-365/>

4 Fin du support MS-Office XP

La fin du support de la suite bureautique Office XP de Microsoft est annoncée pour le 11 juillet 2011, conformément à la politique de support de l'éditeur. Il n'y aura donc plus de correctifs de sécurité après cette date. Les utilisateurs sont donc invités à migrer vers une solution bureautique maintenue.

4.1 Documentation

- Politique de support des produits de Microsoft :
<http://www.microsoft.com/lifecycle>

5 Recommandations pour l'utilisation de RSA SecureID

Après l'attaque qu'elle a subie en mars 2011, la société EMC a indiqué que les intrus avaient visé les données relatives à son produit RSA SecureID, dont le but est de permettre de l'authentification à deux facteurs.

Des sociétés américaines ont ensuite fait état d'attaques contre leurs systèmes d'information, mettant en cause l'utilisation de données relatives aux jetons d'authentification (*tokens*) RSA SecureID.

Face à l'affaiblissement potentiel de cette solution de sécurité, l'ANSSI émet des recommandations dont l'application dépendra de la politique de sécurité et du contexte opérationnel :

- renouveler les éléments sensibles, susceptibles d'avoir été compromis, en particulier les « graines » cryptographiques des jetons. Cette opération est possible pour les versions logicielles. Elle se traduit par le remplacement pour les jetons matériels. La politique de remplacement pourra prendre en compte la qualité de chaque utilisateur et la probabilité qu'il fasse l'objet de tentative d'usurpation d'identité ;
- mettre en garde les utilisateurs de ces produits et le service de support associé contre les pratiques d'ingénierie sociale (filoutage, observation du jeton par un curieux, demande de prêts) ;
- demander le signalement de tout fait suspect de cette nature ou la perte même momentanée d'un jeton ;
- définir des politiques de communication, de support aux utilisateurs et de réaction en cas de détection de l'usurpation d'un compte ou de tentatives d'usurpation ;
- informer les utilisateurs des changements de configuration du système, notamment ceux prévus au titre des autres mesures, via un canal de confiance aisément identifiable par eux et les mettre en garde contre toute communication par un autre canal ;
- dissimuler autant que possible les numéros de série des jetons matériels ;
- se protéger contre l'écoute passive des authentifications légitimes en sécurisant le canal de communication utilisé pour ces authentifications, par exemple à l'aide des protocoles TLS et IPsec ;
- utiliser des facteurs d'authentification complémentaires : activer sur le serveur RSA SecureID la fonctionnalité d'authentification complémentaire par code confidentiel en utilisant la complexité maximale offerte par la solution, soit huit caractères alphanumériques ;
- étudier les possibilités d'utilisation combinée d'autres facteurs d'authentification (certificats...) ;
- détecter les tentatives d'attaques : analyser les journaux afin de détecter les erreurs d'authentification, en particulier celles dues à un jeton invalide, une connexion à une heure inhabituelle, une erreur de synchronisation horaire entre jeton et serveur ou à une mauvaise correspondance entre jeton et utilisateur, etc. ;
- suspendre les accès après 3 à 5 codes confidentiels incorrects ;
- réévaluer les droits octroyés aux utilisateurs authentifiés par cette solution.

Plus globalement, il est nécessaire d'inscrire l'utilisation d'un produit de sécurité dans une architecture de défense en profondeur, et de considérer que l'utilisation d'un tel produit ne dispense pas de toutes les bonnes pratiques en matière de SSI.

6 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/>

7 Rappel des avis émis

Dans la période du 17 au 23 juin 2011, le CERTA a émis les avis suivants :

- CERTA-2011-AVI-361 : Vulnérabilité dans Google Chrome
- CERTA-2011-AVI-362 : Vulnérabilité dans Trend Micro Control Manager
- CERTA-2011-AVI-363 : Vulnérabilité dans Avaya IP Office Manager
- CERTA-2011-AVI-364 : Vulnérabilité dans des produits Blue Coat
- CERTA-2011-AVI-365 : Multiples vulnérabilités dans les produits Mozilla
- CERTA-2011-AVI-366 : Vulnérabilité dans DokuWiki
- CERTA-2011-AVI-367 : Vulnérabilité dans Citrix EdgeSight
- CERTA-2011-AVI-368 : Vulnérabilités dans LibreOffice

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

- CERTA-2011-ALE-003-005 : Vulnérabilité dans Adobe Flash Player, Adobe Reader et Acrobat (annonce des dates de publication des correctifs)

8 Actions suggérées

8.1 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.

8.2 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.

8.3 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.

8.4 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.

8.5 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.

8.6 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.

8.7 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

9 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.

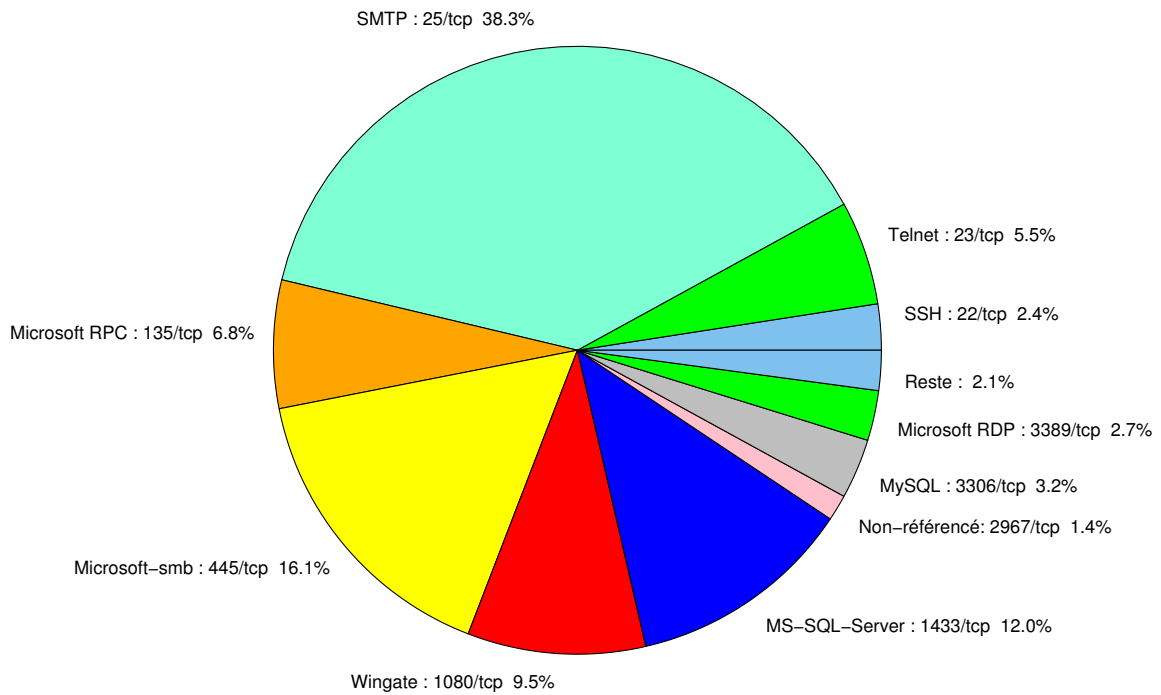


FIG. 1: Répartition relative des ports pour la semaine du 17 au 23 juin 2011

port	pourcentage
25/tcp	38.29
445/tcp	16.06
1433/tcp	12.02
1080/tcp	9.46
80/tcp	7.12
135/tcp	6.8
23/tcp	5.53
3306/tcp	3.19
3389/tcp	2.65
22/tcp	2.44
2967/tcp	1.38
3128/tcp	0.74
4899/tcp	0.53
143/tcp	0.1

TAB. 2: Paquets rejetés

Liste des tableaux

1	Gestion du document	1
2	Paquets rejetés	6

Gestion détaillée du document

24 juin 2011 version initiale.