Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 mai 2012
N° CERTA-2012-ACT-018

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité 2012-018

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-2012-ACT-018`

Gestion du document

Référence	CERTA-2012-ACT-018
Titre	Bulletin d'actualité 2012-018
Date de la première version	04 mai 2012
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-2012-ACT-001.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-2012-ACT-001/

1 Programme tiers et confiance : des écueils

Mises en garde

Le CERTA met régulièrement en garde contre des applications non officielles ou encore contre des greffons ou des extensions provenant de contributeurs extérieurs au projet. Ceci est vrai pour les applications dont le code source n'est pas public, mais également pour les applications à code source ouvert pour lesquelles aucune revue de code sérieuse et méthodique n'a été entreprise.

L'application peut être néfaste dès sa mise en ligne. C'est le cas de certains gratuiciels (*freewares*) qui contiennent de logiciels espions. Ces derniers peuvent remonter des habitudes de navigation à un serveur entrant dans la chaîne d'envoi de publicités ciblées. Sur les boutiques non officielles pour les ordiphones, de nombreuses applications dites bancaires sont en fait de nouvelles formes de filoutage, par interception des données de l'utilisateur.

Mais l'application initiale peut également être anodine lors d'une première version, puis perdre de son innocuité lors d'une mise à jour. Un exemple récent, simplement illustratif, est celui d'une extension pour Firefox dont le nom est *ShowIP*. Jusqu'à la version 1.0, elle affiche l'adresse IP du serveur sur lequel l'internaute est connecté, dans la barre d'état du navigateur. La résolution DNS effectuée par le poste suffit à obtenir l'information d'adressage, qui est ensuite affichée. Lors d'une mise à jour (1.3), le comportement a changé : les adresses des pages visitées

par l'internaute sont envoyées parallèlement vers le serveur d'une société commerciale. De plus, cet envoi n'est même pas chiffré. Il y a une fuite de données qui rend l'application malveillante.

Alertée, la fondation Mozilla a retiré la version intrusive du catalogue des extensions, pour ne proposer que la version 1.0.

Cette réaction est positive, mais elle met en lumière que la publication du programme n'est pas précédée d'une analyse de sécurité.

Recommandations

Le CERTA recommande, tout en respectant la PSSI en vigueur :

- d'appliquer les correctifs de sécurité ;
- d'utiliser des produits maintenus, en vérifiant au maximum leur innocuité, voire, selon les contraintes réglementaires (exemple : RGS) ou des enjeux stratégiques, des produits dont la sécurité a été évaluée (voir section Documentation) ;
- d'établir et d'appliquer une politique prudente d'utilisation des applications et des extensions ;
- de filtrer les flux sortants, de les journaliser et d'exploiter régulièrement ces journaux.

Documentation

- Article Sophos du 01 mai 2012 :
  http://nakedsecurity.sophos.com/2012/05/01/privacy-concern-showip-firefox-add-on/
- Référentiel général de sécurité (RGS), version 1 :
  http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/
- Labellisation des produits de sécurité :
  http://www.ssi.gouv.fr/fr/certification-qualification/
- Bulletin d'actualité du CERTA CERTA-2012-ACT-008 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-008/

2 Les noms de domaine internationalisés

Depuis le 3 mai 2012, il est possible d'enregistrer des noms de domaine sous les extensions opérées par l'AFNIC en utilisant de nouveaux caractères, comprenant notamment des lettres accentuées.

Les extensions de noms de domaine concernées sont `.FR`, `.YT`, `.PM`, `.WF`, `.TF` et `RE`. La liste des 30 nouveaux caractères admis est disponible sur le site de l'AFNIC (cf. section Documentation).

Cette nouveauté, présentée comme un outil d'amélioration de la communication digitale, est susceptible de faciliter la tâche aux *typosquatters*. Le *typosquatting* consiste à enregistrer un nom de domaine très proche d'un nom de domaine cible dans le but de piéger les utilisateurs commettant des erreurs de typographie.

L'AFNIC procède à un enregistrement en deux étapes. Ainsi, du 3 mai 2012 au 3 juillet 2012 a lieu la période d'enregistrement prioritaire, permettant aux titulaires d'un nom de domaine déjà existant de déposer les variantes souhaitées. L'ouverture à tous aura lieu le 3 juillet 2012.

Il sera donc nécessaire d'être d'autant plus vigilant lors de la saisie d'un nom de domaine.

2.1 Documentation :

https://www.afnic.fr/fr/produits-et-services/les-idns.html

3 Suites de la vulnérabilité critique dans Oracle TNS

Dans le bulletin d'actualité CERTA-2012-ACT-017, une vulnérabilité critique affectant *Oracle TNS*, supposée corrigée par l'éditeur, avait été évoquée. *Oracle* a publié, le 30 avril 2012, une alerte de sécurité concernant cette faille (référence CVE-2012-1675). L'éditeur confirme la possibilité d'exploiter la vulnérabilité à distance sans utiliser d'identifiants légitimes. Aucun correctif n'est disponible, seuls des contournements provisoires sont proposés.

Le CERTA recommande l'application des méthodes de contournement proposées par l'éditeur.

Documentation :

- Alerte de sécurité Oracle du 30 avril 2012 :
  http://www.oracle.com/technetwork/topics/security/alert-cve-2012-1675-1608180.html

4 Rappel des avis émis

Dans la période du 27 avril 2012 au 03 mai 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-236 : Vulnérabilité dans certains produits HP
- CERTA-2012-AVI-237 : Multiples vulnérabilités dans VMware
- CERTA-2012-AVI-238 : Multiples vulnérabilités dans HP NonStop
- CERTA-2012-AVI-239 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-240 : Vulnérabilité dans Samba
- CERTA-2012-AVI-241 : Multiples vulnérabilités dans HP SIM
- CERTA-2012-AVI-242 : Vulnérabilités dans SumatraPDF
- CERTA-2012-AVI-243 : Vulnérabilité dans HP SNMP Agents
- CERTA-2012-AVI-244 : Vulnérabilités dans PHP
- CERTA-2012-AVI-245 : Vulnérabilité dans Citrix

5 Actions suggérées

5.1 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.

5.2 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.

5.3 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

Gestion détaillée du document

04 mai 2012 version initiale.