Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 septembre 2012
N° CERTA-2012-ACT-036

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-036

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-036

Gestion du document

Référence	CERTA-2012-ACT-036
Titre	Bulletin d'actualité CERTA-2012-ACT-036
Date de la première version	07 septembre 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.

1 Gestion des mises à jour des ordiphones et tablettes numériques

Les périphériques de types ordiphone (*smartphone*) ou tablette numérique sont conçus dans une logique d'utilisation et de gestion personnelle, peu adaptée aux environnements professionnels.

Ainsi, si la mise à jour des applications installées sur les ordiphones s'obtient facilement grâce aux fonctions de gestion d'applications qu'ils intègrent, connaître le contenu et l'objectif de ces mises à jour pour en qualifier l'importance n'est pas toujours aisé.

De même, réaliser un suivi des mises à jour des systèmes d'exploitation de ces appareils et obtenir la liste des modifications apportées est souvent difficile voire impossible.

En effet, de nombreux intermédiaires (éditeur, constructeur, opérateur, etc.) interviennent avant que la mise à jour n'atteigne l'utilisateur final, rendant très complexe le suivi des versions. D'autant que les mises à jour publiées par les éditeurs ne sont pas forcément déployées par les constructeurs, ni diffusées par les opérateurs.

De plus, les méthodes de déploiement des mises à jour diffèrent pour chaque constructeur (certains imposent l'utilisation d'un logiciel spécifique) et peuvent compliquer leur application. Dans certains cas, l'utilisateur doit effectuer lui-même une opération manuelle afin de vérifier si une mise à jour de sécurité est proposée.

Ces contraintes doivent être prises en compte lors du déploiement de tels périphériques sur un réseau d'entreprise et doivent conduire les responsables des SI à :

- réévaluer régulièrement les menaces ;
- assurer une veille sur les publications des éditeurs, constructeurs et opérateurs, dont les politiques de mise à jour ne sont pas toujours clairement définies et peuvent évoluer sans préavis.

2 Désactivation des greffons inutiles dans les navigateurs

Depuis plusieurs années, les exploitations de vulnérabilités visent particulièrement les applications clientes et notamment les greffons (*plugins*) des navigateurs. Ces greffons permettent d'exécuter du contenu dynamique réalisé par exemple en Java, Flash, PDF ou Silverlight.

Or, si les navigateurs Web sont en général bien intégrés dans les politiques de sécurité des SI, les logiciels tiers sont parfois négligés, alors qu'ils sont également utilisés lors de la navigation et doivent donc être inclus dans les cycles de mise à jour.

De plus, malgré l'importance de garder les navigateurs et leurs composants additionnels à jour, cette bonne pratique ne permet pas toujours de se prémunir des attaques, notamment lors de l'exploitation de vulnérabilités non corrigées (*0day*), comme illustré dernièrement par le greffon Java (CERTA-2012-ALE-005).

Cette situation conduit à la réduction de la robustesse du poste qui peut alors être vulnérable aux codes malveillants propagés par le Web et notamment ceux diffusés par les kits d'exploitation (*exploit kit*).

Le CERTA recommande donc de désactiver les greffons qui ne répondent pas à un besoin métier indispensable.

2.1 Comment désactiver les greffons

Pour désactiver un greffon dans Firefox :

- aller dans le menu "Outils" puis "Modules complémentaires" ;
- choisir l'onglet "plugins" ;
- sélectionner le greffon dans la liste et cliquer sur "Désactiver".

Pour désactiver un greffon dans Internet Explorer :

- aller dans le menu "Outils" puis "Gérer les modules complémentaires" ;
- choisir "Barres d'outils et extensions" ;
- sélectionner le greffon dans la liste et cliquer sur "Désactiver".

Pour désactiver un greffon dans Google Chrome :

- saisir "chrome://plugins/" dans la barre d'adresse ;
- sélectionner le greffon et cliquer sur "Désactiver".

Pour désactiver un greffon dans Safari :

- aller dans "Préférences" dans la barre d'adresse ;
- sélectionner le greffon et cliquer sur "Désactiver".

Pour désactiver un greffon dans Opera :

- saisir "opera:plugins" dans la barre d'adresse ;
- sélectionner le greffon puis cliquer sur "Désactiver".

Active Directory : Dans un domaine Active Directory, les stratégies de groupes (GPO) peuvent être utilisées pour désactiver les greffons dans certains navigateurs, comme Internet Explorer ou Chrome.

2.2 Si la désactivation est impossible

Pour les greffons qui ne peuvent être désactivés, il est conseillé, pour réduire les risques :

- de mettre en place un blocage périmétrique à l'aide d'un serveur mandataire et d'une liste blanche;
- d'activer les stratégies de restrictions logicielles (SRP) (voir CERTA-2010-ACT-014);
- d'utiliser un navigateur exécutant les greffons dans un bac à sable;
- d'appliquer les renforcements de sécurité apportés par EMET (*Enhanced Mitigation Experience Toolkit*) (voir CERTA-2012-ACT-025).

2.3 Documentation

- Alerte CERTA-2012-ALE-005 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ALE-005/index.html
- Bulletin d'actualité CERTA-2012-ACT-025 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-025/index.html
- Bulletin d'actualité CERTA-2010-ACT-014 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2010-ACT-014/index.html

3 Rappel des avis émis

Dans la période du 31 août 2012 au 6 septembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-473 : Vulnérabilité dans Oracle Java
- CERTA-2012-AVI-474 : Multiples vulnérabilités dans IBM AppScan Enterprise and Policy Tester
- CERTA-2012-AVI-475 : Vulnérabilité dans IBM WebSphere Application Server
- CERTA-2012-AVI-476 : Multiples vulnérabilités dans Google Chrome
- CERTA-2012-AVI-477 : Vulnérabilité dans le système SCADA GarrettCom Magnum
- CERTA-2012-AVI-478 : Vulnérabilités dans Asterisk
- CERTA-2012-AVI-479 : Multiples vulnérabilités dans VMware
- CERTA-2012-AVI-480 : Multiples vulnérabilités dans MediaWiki
- CERTA-2012-AVI-481 : Vulnérabilité dans EMC NetWorker
- CERTA-2012-AVI-482 : Vulnérabilités dans Adobe Photoshop CS6
- CERTA-2012-AVI-483 : Vulnérabilité dans PGP Universal Server
- CERTA-2012-AVI-484 : Multiples vulnérabilités dans Typo3
- CERTA-2012-AVI-485 : Multiples vulnérabilités dans Xen
- CERTA-2012-AVI-486 : Vulnérabilité dans le système SCADA InduSoft ISSymbol
- CERTA-2012-AVI-487 : Vulnérabilité dans le système SCADA WAGO SYSTEM 758

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

- CERTA-2012-ALE-005-001 : Vulnérabilité dans Oracle Java (ajout du correctif éditeur, suppression du contournement temporaire)

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 CERTA recommande l'application des correctifs de sécurité.

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

Gestion détaillée du document

07 septembre 2012 version initiale.