Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 novembre 2012
N° CERTA-2012-ACT-046

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2012-ACT-046

1 Sécurité des données et mobilité

Les médias relatent régulièrement des cas de vol ou d'accès illégitimes à des matériels nomades contenant des données sensibles, notamment à l'occasion de déplacements professionnels.
En effet, les données contenues sur des supports amovibles, des ordiphones et des ordinateurs portables sont susceptibles d'être ciblées à des fins d'intelligence économique, d'espionnage, etc.

Afin de se prémunir contre les conséquences d'une perte ou d'un vol, le CERTA rappelle que l'ANSSI a publié un passeport de conseils aux voyageurs édictant les règles fondamentales à respecter dans le cadre d'un déplacement professionnel, parmi lesquelles :

- utiliser du matériel dédié aux missions ;
- sauvegarder au préalable, les données emportées ;
- ne pas se déplacer avec des données sensibles sans lien avec les missions ;
- marquer les appareils d'un signe distinctif pour pouvoir détecter les substitutions ;
- utiliser des solutions de chiffrement.

Concernant ce dernier point, le CERTA ne peut que recommander l'utilisation des solutions de chiffrement certifiées par l'ANSSI, dans le respect de la législation du pays visité sur l'utilisation de la cryptographie.

Documentation

- Passeport de conseils aux voyageurs :
  http://www.securite-informatique.gouv.fr/partirenmission/
- Législation sur l'usage et l'importation de cryptographie à l'étranger :
  http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs_909/

2 Les greffons ciblés par les plates-formes d'exploitation

Une technique classique d'attaque consiste à déposer des codes malveillants sur des sites Internet, puis à attirer les victimes sur ces sites (en usant par exemple de techniques d'ingénierie sociale), dans le but de les compromettre en exploitant une faille présente dans leur navigateur. Ce mode opératoire a beaucoup été utilisé pendant plusieurs années, mais désormais les navigateurs intègrent divers mécanismes de sécurité (notamment de type « bac à sable »). Les attaquants ont donc modifié leur mode opératoire pour cibler les greffons (*plugins*) intégrés aux navigateurs. Ces greffons représentent alors des vecteurs d'attaque intéressants pour les attaquants, puisque le panel des technologies utilisées sur le Web est largement diversifié.

Plusieurs résultats d'études rapportent qu'aujourd'hui la majorité des failles exploitées concernent la technologie Java et les produits Adobe Reader et Flash ; ce phénomène est confirmé par le CERTA dans les incidents qu'il traite. Parallèlement, une autre étude récemment publiée indique que désormais la plupart des plates-formes d'exploitation disponibles ont tendance à privilégier l'intégration de codes d'exploitation pour Java, qui devance à présent les produits Adobe plus massivement concernés les années précédentes.

Le CERTA recommande l'application régulière des correctifs pour ces logiciels tiers, voire leur désactivation complète si aucun correctif n'est disponible ou si leur utilisation n'est pas justifiée. Par exemple, l'intégration d'un greffon PDF au sein d'un navigateur n'est pas indispensable. En le désactivant, la consultation d'un document PDF provoquera son téléchargement. Ce dernier pourra ensuite être lu avec le lecteur PDF local à la machine, après analyse par l'anti-virus de la machine.

Documentation

- Étude de l'évolution des menaces de sécurité par Kaspersky :
  http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012#14
- Évolution des plates-formes d'exploitation :
  http://www.deependresearch.org/2012/11/common-exploit-kits-2012-poster.html

3 Mise à jour mensuelle Microsoft

Lors de la mise à jour mensuelle de Microsoft, six bulletins ont été publiés.

Quatre bulletins sont considérés comme critiques :

- MS12-071 : concernant Microsoft Internet Explorer, cette mise à jour de sécurité corrige trois vulnérabilités permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code à distance avec les droits de l'utilisateur courant ;
- MS12-072 : concernant le porte-documents, cette mise à jour de sécurité corrige deux vulnérabilités permettant à un attaquant, à l'aide d'un porte-documents spécialement conçu, d'exécuter du code à distance avec les droits de l'utilisateur courant ;
- MS12-074 : concernant le *framework* .NET, cette mise à jour de sécurité corrige cinq vulnérabilités dont la plus grave permet à un attaquant, s'il arrive à persuader un utilisateur d'utiliser un fichier de configuration de proxy spécialement conçu, d'exécuter du code à distance en l'injectant dans l'application en cours d'exécution ;
- MS12-075 : concernant le noyau Windows, cette mise à jour de sécurité corrige trois vulnérabilités permettant à un attaquant :
  - d'élever ses privilèges grâce à une application spécialement conçue ;
  - d'exécuter du code à distance avec des droits système à l'aide d'un fichier de police TrueType spécialement conçu.

Un bulletin est considéré comme important (MS12-076) et concerne Microsoft Excel. Cette mise à jour de sécurité corrige quatre vulnérabilités permettant à un attaquant, à l'aide d'un document Excel spécialement conçu, d'exécuter du code à distance avec les droits de l'utilisateur courant.

Un bulletin est considéré comme modéré (MS12-073) et concerne Microsoft IIS 7.0. Cette mise à jour de sécurité corrige deux vulnérabilités permettant la divulgation d'informations :

- de connexion (nom d'utilisateur / mot de passe) contenues dans le fichier journal non protégé ;
- par le biais de commandes FTP spécialement conçues.

En dehors de la vulnérabilité d'envoi de commandes spécialement conçues corrigée par le bulletin MS12-073, aucune de ces vulnérabilités n'avait été divulguée publiquement précédemment. D'après les observations de Microsoft, aucune attaque exploitant ces vulnérabilités n'a été révélée avant la publication de ces bulletins.

Le CERTA recommande l'application de ces mises à jour dès que possible.

Documentation

- Avis CERTA-2012-AVI-644 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-644/
- Avis CERTA-2012-AVI-645 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-645/

- Avis CERTA-2012-AVI-646 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-646/
- Avis CERTA-2012-AVI-647 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-647/
- Avis CERTA-2012-AVI-648 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-648/
- Avis CERTA-2012-AVI-649 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-AVI-649/
- Synthèse des bulletins de sécurité Microsoft du mois de novembre 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-nov

4 Rappel des avis émis

Dans la période du 09 au 15 novembre 2012, le CERTA a émis les publications suivantes :

- CERTA-2012-AVI-635 : Multiples vulnérabilités dans Apple Quicktime
- CERTA-2012-AVI-636 : Multiples vulnérabilités dans LibreOffice
- CERTA-2012-AVI-637 : Multiples vulnérabilités dans Cisco Ironport
- CERTA-2012-AVI-638 : Vulnérabilité dans VLC
- CERTA-2012-AVI-639 : Vulnérabilité dans Joomla!
- CERTA-2012-AVI-640 : Vulnérabilité dans WebSphere MQ
- CERTA-2012-AVI-641 : Multiples vulnérabilités dans TYPO3
- CERTA-2012-AVI-642 : Multiples vulnérabilités dans VMware Workstation et Player
- CERTA-2012-AVI-643 : Vulnérabilité dans Ruby
- CERTA-2012-AVI-644 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2012-AVI-645 : Multiples vulnérabilités dans Internet Explorer
- CERTA-2012-AVI-646 : Multiples vulnérabilités dans le Shell Windows
- CERTA-2012-AVI-647 : Multiples vulnérabilités dans Microsoft Internet Information Services
- CERTA-2012-AVI-648 : Multiples vulnérabilités dans Microsoft NET Framework
- CERTA-2012-AVI-649 : Multiples vulnérabilités dans les pilotes en mode noyau de Windows
- CERTA-2012-AVI-650 : Multiples vulnérabilités dans Xen
- CERTA-2012-AVI-651 : Multiples vulnérabilités dans Citrix XenServer
- CERTA-2012-AVI-652 : Multiples vulnérabilités dans SAP NetWeaver
- CERTA-2012-AVI-653 : Multiples vulnérabilités dans Moodle
- CERTA-2012-AVI-654 : Multiples vulnérabilités dans Bugzilla
- CERTA-2012-AVI-655 : Multiples vulnérabilités dans IBM Java SDK

Gestion détaillée du document

16 novembre 2012 version initiale.