Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 juin 2013
N° CERTA-2013-ACT-024

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-024

1 Problèmes liés aux droits administrateur

Le CERTA a récemment été amené à traiter un incident relatif à l'utilisation de logiciels contrefaits sur un poste de travail.

Les privilèges d'administration octroyés de manière abusive et non contrôlée à un utilisateur, lui autorisent le téléchargement et l'installation de logiciels contrefaits ou piratés à l'insu des administrateurs.

Au-delà du caractère illégal que constitue cette pratique, l'utilisateur expose son poste de travail à des infections par des codes malveillants subrepticement intégrés au logiciel pirate.

La mise en place des règles de base répertoriées dans le guide de l'hygiène informatique telles que l'interdiction de donner aux utilisateurs des privilèges d'administration ou encore la sensibilisation des utilisateurs à la manipulation de programmes d'origines inconnues, permettra d'accroitre le niveau de sécurité du système tout en limitant les pratiques à risque.

Documentation

- Guide d'hygiène d'informatique :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

2 Publication par Microsoft d'un *Fix it* pour désactiver Java dans IE

Java représente toujours l'un des vecteurs de compromission les plus utilisés. Son greffon intégré dans les navigateurs Web étant particulièrement exposé, le CERTA recommande régulièrement de le désactiver lorsqu'il n'est pas nécessaire.

Cependant, désactiver complètement Java dans Internet Explorer est assez complexe et nécessite la mise en place de bits d'arrêts dans la base de registre. Microsoft a donc publié recemment un *Fix it* permettant de désactiver simplement, complètement et durablement Java dans Internet Explorer.

Le CERTA recommande donc :

- de supprimer entièrement l'environnement Java des postes où il n'est pas nécessaire ;
- d'appliquer les recommandations du guide ANSSI ;
- d'appliquer ce *Fix It* sur les postes qui n'utilisent pas le greffon mais où l'environnement d'exécution Java est nécessaire, par exemple pour des applications locales.

Secrétariat général de la défense et de la sécurité nationale – ANSSI – COSSI – CERTA
51, bd de La Tour-Maubourg **Tél.**: 01 71 75 84 50 **Web**: http://www.certa.ssi.gouv.fr
75700 Paris 07 SP **Fax**: 01 71 75 84 70 **Mél** : certa-svp@certa.ssi.gouv.fr

Documentation

- *How to disable the Java web plug-in in Internet Explorer* :
  http://support.microsoft.com/kb/2751647/en-us
- Recommandations de sécurité relatives aux environnements d'exécution Java sur les postes de travail Microsoft Windows :
  http://www.ssi.gouv.fr/recos-securite-poste-java

3 Mise à jour mensuelle Microsoft

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

Un bulletin est considéré comme critique. Il s'agit de la vulnérabilité MS13-047 qui concerne Microsoft Internet Explorer, cette mise à jour corrige dix-neuf vulnérabilités permettant à un attaquant, à l'aide d'une page Web ou d'un document spécialement conçu, d'exécuter du code arbitraire à distance.

Quatre bulletins sont considérés comme importants, ils concernent :

- une vulnérabilité dans le noyau Microsoft Windows (MS13-048) ;
- une vulnérabilité dans le système TCP/IP de Microsoft Windows (MS13-049) ;
- une vulnérabilité dans le spouleur d'impression Microsoft Windows (MS13-050) ;
- une vulnérabilité dans Microsoft Office (MS13-051).

Microsoft a connaissance d'attaques ciblées visant à exploiter la vulnérabilité corrigée par le bulletin MS13-051. Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de juin 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-jun
- Publication de Microsoft « MS13-051: Get Out of My Office! » :
  http://blogs.technet.com/b/srd/archive/2013/06/11/ms13-051-get-out-of-my-office.aspx

4 Rappel des avis émis

Dans la période du 07 au 13 juin 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-345 : Vulnérabilité dans Drupal
- CERTA-2013-AVI-346 : Multiples vulnérabilités dans PHP
- CERTA-2013-AVI-347 : Multiples vulnérabilités dans Wireshark
- CERTA-2013-AVI-348 : Vulnérabilité dans Adobe Flash Player
- CERTA-2013-AVI-349 : Vulnérabilité dans VMware vCenter Chargeback Manager
- CERTA-2013-AVI-350 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-351 : Vulnérabilité dans le noyau Microsoft Windows
- CERTA-2013-AVI-352 : Vulnérabilité dans le système TCP/IP de Microsoft Windows
- CERTA-2013-AVI-353 : Vulnérabilité dans le spouleur d'impression Microsoft Windows
- CERTA-2013-AVI-354 : Vulnérabilité dans Microsoft Office
- CERTA-2013-AVI-355 : Multiples vulnérabilités dans le noyau Linux de Red Hat

Gestion détaillée du document

14 juin 2013 version initiale.