Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mars 2013
N° CERTA-2013-ACT-011

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-011

1 Sécurité logicielle et défense en profondeur

La semaine dernière s'est déroulée à Vancouver (Canada) la dernière édition de la compétition « Pwn2Own ». Cette compétition propose aux concurrents, généralement des sociétés spécialisées en sécurité informatique, de démontrer leur savoir-faire dans le domaine de l'exploitation des vulnérabilités des navigateurs Web, ainsi que de leurs greffons et autres extensions.

Cette année, des failles inédites ont été démontrées sur les logiciels suivants :

- Navigateurs Internet :
  - Google Chrome (sur Windows 7) ;
  - Microsoft Internet Explorer 10 (sur Windows 8) ;
  - Microsoft Internet Explorer 9 (sur Windows 7) ;
  - Mozilla Firefox (sur Windows 7) ;
- Greffons (pour Internet Explorer 9 sur Windows 7) :
  - Adobe Reader XI ;
  - Adobe Flash ;
  - Oracle Java.

Ces failles ont été démontrées sur les versions les plus à jour des systèmes et produits au moment de l'épreuve.

Cette illustration montre, encore une fois, que même s'il est à jour, un composant logiciel complexe n'est jamais exempt de failles permettant à un attaquant de prendre le contrôle d'un système.

Si la mise à jour des composants logiciels reste une étape primordiale dans la sécurisation d'un SI, il est nécessaire d'aller plus loin et de mettre en place une stratégie de défense en profondeur, afin d'empêcher un attaquant ayant compromis un poste de rebondir sur les autres machines du réseau.
Le guide d'hygiène informatique disponible sur le site de l'ANSSI (*cf. Documentation*) regroupe un ensemble de conseils permettant de jeter les bases d'une telle politique.

Documentation

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

2 Keylogger matériel et sécurité physique

Récemment, le CERTA a été amené à traiter un incident impliquant l'utilisation d'un *keylogger* (enregistreur de frappes clavier) matériel. Le dispositif branché entre le poste et le clavier permettait la collecte de l'ensemble des frappes clavier réalisées par les utilisateurs. Bien que la détection de ce type de piège autrement que par un contrôle visuel soit difficile, il est important de prendre conscience de la pertinence de cette menace.

Pour y pallier, le CERTA recommande :

- la mise en place d'une politique de sécurité physique : comme cela est indiqué dans le guide d'hygiène informatique de l'ANSSI, il est impératif d'utiliser des mécanismes et procédures robustes de contrôle d'accès aux locaux ;
- la sensibilisation des utilisateurs et techniciens informatiques aux risques SSI, en incluant les risques liés aux compromissions physiques des postes. À ce titre, il est pertinent de recommander la vérification régulière de l'intégrité physique des postes de travail.

3 Périphériques USB - vulnérabilité MS13-027

Cette semaine, Microsoft a publié un correctif concernant plusieurs vulnérabilités permettant à un attaquant d'exécuter du code arbitraire en mode noyau. Selon Microsoft, ces vulnérabilités peuvent être facilement exploitables au moyen d'un périphérique USB spécialement conçu. S'il dispose d'un accès physique à la machine, l'attaquant peut utiliser cette vulnérabilité pour prendre le contrôle du système avec les droits administrateur sans disposer de compte sur la machine.

La sécurité des systèmes déconnectés repose essentiellement sur la gestion d'accès physique. Dans cette optique, un filtrage des périphériques USB autorisés est souvent mis en place. Celui-ci repose sur une liste de « VendorID » et/ou de « ProductID ». Ces protections, bien que nécessaires, ont leurs limites et ne peuvent garantir un filtrage efficace, car les informations (« VendorID » et « ProductID ») peuvent être usurpées. De plus, il est important de noter que face à la vulnérabilité MS13-027, ces solutions ne sont pas suffisantes.

D'une manière générale, afin de se protégér contre ce type de vulnérabilités pour les systèmes les plus critiques, il doit être envisagé de désactiver physiquement les ports USB et d'utiliser des alternatives pour le transfert de données (CD-ROM, graveur, . . .).

Enfin, il est probable que cette vulnérabilité soit également présente sur des systèmes Microsoft obsolètes (Windows 2000, XP SP1 et SP2 . . .) pour lesquels aucun correctif ne sera publié.

Le CERTA recommande de déployer cette mise à jour sur l'ensemble des stations vulnérables et de veiller à appliquer une politique de contrôle d'accès physique rigoureuse (cf. Guide d'hygiène informatique de l'ANSSI).

Documentation

- Avis CERTA CERTA-2013-AVI-183 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-183/

4 Mise à jour mensuelle Microsoft

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

Quatre bulletins sont considérés comme critiques par Microsoft :

- MS13-021, qui concerne Microsoft Internet Explorer, corrige neuf vulnérabilités permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code arbitraire à distance ;
- MS13-022, qui concerne Microsoft Silverlight, corrige une vulnérabilité permettant à un attaquant, à l'aide d'une page Web spécialement conçue, d'exécuter du code arbitraire à distance ;
- MS13-023, qui concerne Microsoft Visio Viewer 2010, corrige une vulnérabilité permettant à un attaquant, à l'aide d'un fichier spécialement conçu, d'exécuter du code arbitraire à distance ;
- MS13-024, qui concerne Microsoft Microsoft SharePoint, corrige quatre vulnérabilités permettant à un attaquant, à l'aide de requêtes spécialements conçues, d'élever ses privilèges ;

Le CERTA recommande l'application de ces correctifs dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de mars 2013 :
  http://technet.microsoft.com/security/bulletin/ms13-mar

5 Rappel des avis émis

Dans la période du 08 au 14 mars 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-171 : Vulnérabilité dans les produits Mozilla
- CERTA-2013-AVI-172 : Vulnérabilité dans Google Chrome
- CERTA-2013-AVI-173 : Multiples vulnérabilités dans Wireshark
- CERTA-2013-AVI-174 : Vulnérabilité dans HP ServiceCenter
- CERTA-2013-AVI-175 : Vulnérabilité dans HP LaserJet Pro
- CERTA-2013-AVI-176 : Multiples vulnérabilités dans Adobe Flash Player et AIR
- CERTA-2013-AVI-177 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-178 : Vulnérabilité dans Microsoft Silverlight
- CERTA-2013-AVI-179 : Vulnérabilité dans Microsoft Visio Viewer 2010
- CERTA-2013-AVI-180 : Multiples vulnérabilités dans Microsoft SharePoint
- CERTA-2013-AVI-181 : Vulnérabilité dans Microsoft OneNote
- CERTA-2013-AVI-182 : Vulnérabilité dans Microsoft Office Outlook
- CERTA-2013-AVI-183 : Multiples vulnérabilités dans Microsoft Windows
- CERTA-2013-AVI-184 : Multiples vulnérabilités dans NVIDIA
- CERTA-2013-AVI-185 : Vulnérabilité dans Squid Proxy

Gestion détaillée du document

15 mars 2013 version initiale.