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 novembre 2013
N° CERTA-2013-ACT-046

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTA-2013-ACT-046**

## 1 - Une petite parcelle d'Internet s'éteint

Le CERTA tient à rendre hommage à l'ingénieur chercheur en sécurité informatique Cédric "Sid" Blancher, décédé soudainement le 10 Novembre 2013 suite à un accident de parachutisme.

Respecté par de nombreux experts en sécurité informatique, Cédric Blancher a contribué à faire progresser la sécurité des systèmes d'information avec beaucoup de pédagogie et un savoir-faire largement reconnu, notamment dans le domaine de la sécurité des réseaux. Doté d'un franc-parler et d'un pragmatisme qui le caractérisaient, il a notamment :

- dispensé de nombreuses interventions à des écoles d'ingénieur, des universités ou des entreprises ;
- publié et contribué à de nombreux articles pour des revues spécialisées ou sur son blog ;
- participé en tant que conférencier à de très nombreuses conférences spécialisées ;
- organisé des événements afin de sensibiliser et promouvoir la sécurité des systèmes d'information.

Le CERTA tient à présenter toutes ses condoléances à sa famille et à ses proches.

**Liens**

- Blog de Cédric Blancher "Ma petite parcelle d'Internet" :
  http://sid.rstack.org/blog/index.php
- Articles de Cédric Blancher :
  http://sid.rstack.org/articles
- Présentations de Cédric Blancher :
  http://sid.rstack.org/pres/

## 2 - Rappel sur la vulnérabilité critique CVE-2013-3906 dans un composant graphique de Microsoft

La semaine dernière, le CERTA a diffusé l'alerte CERTA-2013-ALE-007 concernant une vulnérabilité majeure dans un composant graphique de Microsoft.

Cette vulnérabilité permet, au travers un fichier embarquant une image TIFF spécialement conçue, une exécution de code arbitraire à distance. Le CERTA rappelle qu'elle est déjà publique et largement exploitée par les attaquants.

Puisque la mise à jour mensuelle de Microsoft de ce mois-ci ne corrige pas cette vulnérabilité, le CERTA recommande l'application de la solution de contournement préconisée par Microsoft : la désactivation du codec TIFF en créant la clef de registre HKLM\SOFTWARE\Microsoft\Gdiplus\DisableTIFFCodec=1 ou en applicant le Fix-it de Microsoft.

Dans le cas où cette recommandation ne serait pas applicable, deux techniques de défense en profondeur sont conseillées par Microsoft :

- la mise en place d'EMET (à partir de la version 3.0) ;
- l'utilisation du mode Protected View de Microsoft Office (par défaut dans la version 2010) et le blocage des contrôles ActiveX dans les documents Microsoft Office.

Ces mesures ne corrigent pas la vulnérabilité mais elles permettent d'empêcher son exploitation par un attaquant.

**Documentation:**

- Bulletin d'alerte nunéro 7 du 6 novembre 2013 du CERTA :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-007/index.html
- Bulletin de sécurité Microsoft 2896666 du 05 novembre 2013 :
  http://technet.microsoft.com/en-us/security/advisory/2896666
- Fix-it de Microsoft :
  https://support.microsoft.com/kb/2896666
- EMET 4.1 :
  http://www.microsoft.com/en-us/download/details.aspx?id=41138
- Guide de sécurité "Vulnérabilités 0-day : prévention et bonnes pratiques" :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/vulnerabilites-0-day-prevention-et-bonnes-pratiques.html

# 3 - Mise à jour mensuelle Microsoft

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

Les trois premiers bulletins sont considérés comme critiques :

- MS13-088 qui concerne *Internet Explorer*, cette mise à jour corrige dix vulnérabilités ;
- MS13-089 qui concerne le composant GDI de Windows, cette mise à jour corrige une vulnérabilité ;
- MS13-090 qui concerne un *ActiveX*, cette mise à jour corrige une vulnérabilité.

Toutes ces vulnérabilités peuvent mener un attaquant à exécuter du code arbitraire à distance. Le correctif MS13-090 corrige la vulnérabilité CVE-2013-3918 qui est activement exploitée.

Cinq bulletins sont considérés comme importants :

- MS13-091 qui concerne *Office*, cette mise à jour corrige trois vulnérabilités qui peuvent mener à une exécution de code à distance ;
- MS13-092 qui concerne le noyau *Hyper-V*, cette mise à jour corrige une vulnérabilité qui peut mener à une élévation de privilèges ;
- MS13-093 qui concerne le pilote de gestion des sockets de Microsoft Windows, cette mise à jour corrige une vulnérabilité qui peut mener à une divulgation d'informations ;
- MS13-094 qui concerne *Outlook*, cette mise à jour corrige une vulnérabilité qui peut mener à une divulgation d'informations ;
- MS13-095 qui est liée aux signatures numériques de Microsoft Windows, cette mise à jour corrige une vulnérabilité qui peut mener à un déni de service.

Microsoft a également publié une mise à jour en version 4.1 de son outil de protection en profondeur `EMET`. Cette mise à jour facilite le déploiement de l'outil à grande échelle.

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

**Documentation**

- Synthèse des bulletins de sécurité Microsoft du mois de novembre 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-nov
- Bulletin Microsoft concernant EMET 4.1 :
  http://blogs.technet.com/b/srd/archive/2013/11/12/introducing-enhanced-mitigation-experience-toolkit-emet-4-1.aspx

# 4 - Compromission d'Adobe et fuite de mots de passe

Le 3 octobre 2013, Adobe a révélé un incident de sécurité dans son infrastructure, engendrant notamment la récupération de sa base de données clients par une personne malintentionnée.

## Description de la compromission

Adobe a été victime début octobre d'une intrusion sur son système d'information. Elle a permis à l'attaquant d'accéder aux codes sources de produits Adobe, mais également à des données personnelles de clients. Parmi ces données se trouve la base de données des utilisateurs de ses services. Fin octobre 2013, une copie de cette base de données, contenant les informations de plus de 150 millions d'utilisateurs, a été rendue public sur Internet. Cette base contient plusieurs informations dont :

- l'adresse de courrier électronique ;
- le mot de passe chiffré puis encodé en base64 ;
- un indice permettant de retrouver le mot de passe.

L'analyse de ces informations met en évidence un certain nombre de mauvaises pratiques quant à la gestion de données sensibles :

- l'indication de mot de passe est en clair : cet indice, fourni librement par l'utilisateur lors de son inscription, est parfois bien trop explicite sur le mot de passe (par exemple : « mon mot de passe est 123456 ») ;
- les mots de passe sont chiffrés à l'aide d'un chiffrement réversible (a priori 3DES) rendant possible la découverte du mot de passe clair, à condition de disposer de la clé de chiffrement stockée sur le serveur ;
- le mode de chiffrement des mots de passe est ECB, ce qui provoque des collisions sur le chiffré ;
- la transformation des mots de passe n'est pas perturbée par l'utilisation d'un sel aléatoire.

## Recommandations

Le CERTA recommande d'appliquer certaines bonnes pratiques concernant la sécurisation des mots de passe sur un site web :

- les mots de passe doivent être stockés sous une forme transformée par une fonction cryptographique à sens unique (fonction de hachage) et lente à calculer telle que PBKDF2 ;
- la transformation des mots de passe doit faire intervenir un sel aléatoire pour empêcher une attaque par tables pré-calculées ;
- une politique de complexité doit être appliquée pour assurer la robustesse des mots de passe ;
- l'utilisation d'indices doit être évitée (si nécessaires, ils doivent alors être stockés sous forme chiffrée).

Le CERTA recommande aux utilisateurs concernés par cette compromission de changer leur mot de passe au plus vite.

Le CERTA recommande également de choisir un mot de passe unique et complexe pour chacun des comptes utilisés sur différents sites Internet. Ainsi, la compromission d'un site en particulier n'aura pas d'impact sur la confidentialité des autres mots de passe.

Plutôt que de mémoriser l'ensemble de ces mots de passe uniques, il est recommandé d'utiliser un gestionnaire tel que *KeePass* (certifié CSPN) qui est capable de générer des mots de passe respectant les contraintes énoncées précédemment et de protéger ceux-ci à l'aide d'un mot de passe principal.

Le respect de ces mesures permet de se prémunir d'un certain nombre de risques dans le cas où la base de mots de passe se retrouverait accessible par un attaquant.

Pour mémoire, l'ANSSI a publié sur son site des recommandations sur la sécurisation des sites web et sur la sécurité des mots de passe.

#### Documentation

- Alerte de sécurité d'Adobe :
  http://helpx.adobe.com/fr/x-productkb/policy-pricing/customer-alert.html
- Déclaration d'Adobe :
  http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html
- Recommandations pour la sécurisation des sites web :
  http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html

– Recommandations de sécurité relatives aux mots de passe :
http://www.ssi.gouv.fr/mots-de-passe
– Site de l'éditeur *KeePass* :
http://keepass.info/
– Certification CSPN de *KeePass* :
http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-certifies-cspn/certificat_cspn_2010_07.html

# 5 - Rappel des avis émis

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

– CERTA-2013-AVI-621 : Vulnérabilité dans IBM Lotus Sametime WebPlayer
– CERTA-2013-AVI-622 : Vulnérabilité dans ISC BIND
– CERTA-2013-AVI-623 : Vulnérabilité dans OpenSSH
– CERTA-2013-AVI-624 : Multiples vulnérabilités dans Samba
– CERTA-2013-AVI-625 : Vulnérabilité dans Xen
– CERTA-2013-AVI-626 : Multiples vulnérabilités dans SPIP
– CERTA-2013-AVI-627 : Multiples vulnérabilités dans Microsoft Internet Explorer
– CERTA-2013-AVI-628 : Vulnérabilité dans Microsoft GDI
– CERTA-2013-AVI-629 : Vulnérabilité dans Microsoft ActiveX
– CERTA-2013-AVI-630 : Multiples vulnérabilités dans Microsoft Office
– CERTA-2013-AVI-631 : Vulnérabilité dans Microsoft Hyper-V
– CERTA-2013-AVI-632 : Vulnérabilité dans le pilote de gestion des sockets de Microsoft Windows
– CERTA-2013-AVI-633 : Vulnérabilité dans Microsoft Outlook
– CERTA-2013-AVI-634 : Vulnérabilité liée aux signatures numériques de Microsoft Windows
– CERTA-2013-AVI-635 : Multiples vulnérabilités dans Google Chrome
– CERTA-2013-AVI-636 : Multiples vulnérabilités dans Adobe Flash Player
– CERTA-2013-AVI-637 : Multiples vulnérabilités dans Cisco Prime Data Center Network Manager
– CERTA-2013-AVI-638 : Vulnérabilité dans IBM WebSphere Virtual Enterprise

# Gestion détaillée du document

**15 novembre 2013** version initiale.