Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 février 2013
N° CERTA-2013-ACT-008

**Affaire suivie par :**
CERTA

# BULLETIN D'ACTUALITÉ

**Objet : Bulletin d'actualité CERTA-2013-ACT-008**

| | |
|---|---|
| Conditions d'utilisation de ce document : | `http://www.certa.ssi.gouv.fr/certa/apropos.html` |
| Dernière version de ce document : | `http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-008` |

## 1 Recommandations de sécurité pour les dispositifs de vidéosurveillance

L'ANSSI a récemment publiqué une note technique intitulée *Recommandations de sécurité pour la mise en oeuvre de dispositifs de vidéoprotection*.

Ce document décrit un ensemble de mesures et de principes, dont la mise en oeuvre vise à contrer les vulnérabilités des dispositifs de vidéo surveillance, au travers des thématiques suivantes :

- analyse des menaces ;
- architecture du réseau support ;
- choix et configuration des équipements de vidéoprotection ;
- sécurité du centre de supervision ;
- problématiques de signaux compromettants ;
- aspects contractuels en cas de sous-traitance.

### Documentation

- Recommandations de sécurité pour la mise en oeuvre de dispositifs de vidéoprotection
  http://www.ssi.gouv.fr/IMG/pdf/videoprotection_notetechnique_anssi.pdf

## 2 Sécurisation de Adobe Reader sous environnement Microsoft Windows

La semaine dernière, le CERTA a diffusé l'alerte CERTA-2013-ALE-002 concernant un exploit qui utilisait deux vulnérabilités majeures dans Adobe Reader et Acrobat. Ces vulnérabilités ont été corrigées mais le risque d'un nouveau « 0-day » ne peut être écarté. Cet article présente quelques recommandations pour durcir la configuration du lecteur PDF d'Adobe dans l'environnement Microsoft Windows et réduire les risques de compromission au moyen de fichiers PDF spécialement conçus.

Le CERTA recommande :

- de déployer la dernière version, apportant des améliorations de la configuration et davantage de mécanismes de sécurité ;
- d'activer le mode protégé (sandbox) et la protection renforcée (restriction sur l'exécution des scripts ). Il faut également recommander d'activer la création d'un fichier journal pour le mode protégé et la protection renforcée ;
- de désactiver des fonctionnalités inutilisées comme :
  - le moteur JavaScript,

– les opérations multimedia (catégorie « fiabilité multimedia » ),
– les fichiers PDF joints et les accès à Internet des fichiers PDF (Gestionnaire des approbations).

Ces paramètres doivent être déployés de préférence par GPO (fichiers ADMX fournis par Adobe) afin que tout le système d'information soit couvert de manière homogène.

Même si le moteur JavaScript est désactivé par l'administrateur, il est activable temporairement par l'utilisateur lors de l'ouverture d'un fichier PDF contenant du code JavaScript. Des messages de sensibilisation doivent donc être diffusés pour éviter ce comportement.

Ces mesures de durcissement d'Adobe Reader doivent être complétées par des mesures génériques relatives aux systèmes Microsoft Windows :

– utiliser une version récente de Microsoft Windows (7 ou 8), pour bénéficier des améliorations au niveau des mécanismes de sécurité (notamment de sandbox) ;
– utiliser une compte non privilégié (activation de UAC depuis Microsoft Windows Vista).

Enfin, quelques mesures génériques relatives à un parc Microsoft Windows peuvent être mises en place pour réduire les conséquences de la compromission d'un poste de travail :

– créer des postes dédiées à l'administration, distinct des postes bureautiques standards ;
– activer le pare-feu local des postes de travail pour empêcher les connexions entrantes depuis un autre poste de travail ;
– créer des comptes dédiés à l'administration des postes de travail et pas plus privilégiés.

Le CERTA souligne également que ces éléments de configuration doivent être préalablement testés et qualifiés avant d'être appliqués.

### Documentation

– Alerte CERTA-2013-ALE-002 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-002/

## 3 Oracle Java version 7 mise à jour 15

Le 19 février 2013, Oracle a publié la version 7 mise à jour 15 de Java (CERTA-2013-AVI-142). Elle corrige 6 vulnérabilités et s'agit d'une mise à jour « hors cycle » de Oracle. Cette mise à jour corrige entre autre la première vulnérabilité évoquée dans l'alerte (CERTA-2013-ALE-001). Cette vulnérabilité n'avait pas été corrigée dans les mises à jour 11 et 13 de Oracle Java . Elle permettait de charger une classe dans l'espace de noms (namespace) système depuis l'espace de nom « Applet » au moyen de la méthode « findClass » de la classe « MBeanInstantiator ». Avec la mise à jour 15 de Oracle Java, les vulnérabilités utilisées dans les codes d'exploitation publics sont maintenant toutes corrigées.

Le CERTA recommande d'appliquer la mise à jour 15 le plus rapidement possible lorsque la désactivation de Java dans le navigateur n'est pas possible et de suivre les règles de base de sécurité qui sont :

– de prendre garde aux liens qui sont dans les courriels ;
– de faire preuve de vigilance lorsque vous consultez des sites Web non vérifiés.

Pour plus d'information, nous vous conseillons de lire le bulletin d'actualité 006 ( CERTA-2013-ACT-006 ).

### Documentation

– Bulletin de sécurité Oracle JavaCPUFeb2013update du 19 février 2013 :
http://www.oracle.com/technetwork/topics/security/javacpufeb2013update-1905892.html
– Avis CERTA-2013-AVI-142 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-142/
– Alerte Oracle Java CERTA-2013-ALE-001 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-001/
– Bulletin d'actualité CERTA-2013-ACT-006 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-006/

# 4 Exploitation de vulnérabilités visant la plate-forme Max OS X

Comme l'a illustré le code malveillant « Flashback » l'année dernière, la plate-forme Mac OS X est également la cible de codes d'exploitation. Ainsi à l'instar d'autres systèmes, celle-ci a récemment été sujette aux vulnérabilités Java largement utilisées par des codes malveillants ou des plates-formes d'exploitation. Ces vulnérabilités ont été corrigées dans la nouvelle version Java 1.6.0_41 maintenue par Apple pour ses systèmes d'exploitation OS X 10.6 et Mountain Lion. Ce dernier correctif désactive désormais par défaut le greffon Java pour l'exécution d'applet au sein du navigateur, ce qui réduit immédiatement la surface d'exploitation pour l'attaquant. Il est désormais à la charge de l'utilisateur d'installer le greffon distribué par Oracle.

Des attaques ont déjà été relatées concernant d'autres produits de la plate-forme Mac OS X. Ce fut par exemple le cas de campagnes d'attaques visant certaines communautés l'année dernière : des codes d'exploitation visant Microsoft Office pour Mac ont été utilisés afin de délivrer les charges malveillantes.

L'exposition de Mac OS X aux attaques n'est pas marginale: ce système possède des vulnérabilités comme n'importe quel autre système d'exploitation. Ainsi les précautions de mises à jour habituellement préconisées par le CERTA sont applicables de la même manière sur cette plate-forme.

### Documentation

- Bulletin d'actualité CERTA-2012-ACT-046 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2012-ACT-046/
- Avis CERTA-2013-AVI-142 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-142/

# 5 Rappel des avis émis

Dans la période du 15 février au 22 février 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-131 : Vulnérabilité dans Xen oxenstored
- CERTA-2013-AVI-132 : Vulnérabilité dans Xen
- CERTA-2013-AVI-133 : Multiples vulnérabilités dans Ruby on Rails
- CERTA-2013-AVI-134 : Multiples vulnérabilités dans IBM WebSphere Message Broker
- CERTA-2013-AVI-135 : Multiples vulnérabilités dans Symantec Encryption Desktop
- CERTA-2013-AVI-136 : Multiples vulnérabilités dans Google Chrome
- CERTA-2013-AVI-137 : Vulnérabilité dans les systèmes SCADA Siemens CP 1616 et CP 1604
- CERTA-2013-AVI-138 : Multiples vulnérabilités dans IBM InfoSphere DataStage
- CERTA-2013-AVI-139 : Multiples vulnérabilités dans les produits IBM
- CERTA-2013-AVI-140 : Multiples vulnérabilités dans IBM Data Studio Help System
- CERTA-2013-AVI-141 : Multiples vulnérabilités dans les produits Hitachi
- CERTA-2013-AVI-142 : Multiples vulnérabilités dans Oracle Java
- CERTA-2013-AVI-143 : Multiples vulnérabilités dans Apple OS X et Mac OS X
- CERTA-2013-AVI-144 : Multiples vulnérabilités dans Mozilla Firefox
- CERTA-2013-AVI-145 : Multiples vulnérabilités dans Oracle Solaris

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

- CERTA-2013-ALE-002-002 : Vulnérabilités dans Adobe Reader et Acrobat (ajout du correctif et fermeture alerte)

# Gestion détaillée du document

**22 février 2013** version initiale.