Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2013
N° CERTA-2013-ACT-037

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-037

Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2013-ACT-037

1 Mise à jour mensuelle Microsoft

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

Quatre bulletins sont considérés comme critiques :

- MS13-067 qui concerne Microsoft SharePoint Server, cette mise à jour corrige plusieurs vulnérabilités, la plus grave pourrait permettre l'exécution de code à distance dans le contexte du compte de service W3WP, si un attaquant envoyait au serveur concerné du contenu spécialement conçu ;
- MS13-068 qui concerne Microsoft Outlook, cette mise à jour corrige une vulnérabilité qui pourrait permettre l'exécution de code à distance si un utilisateur ouvrait ou prévisualisait un message electronique spécialement conçu ;
- MS13-069 qui concerne Microsoft Internet Explorer, cette mise à jour corrige plusieurs vulnérabilités, les plus graves pourraient permettre l'exécution de code à distance si un utilisateur affichait à l'aide d'Internet Explorer une page Web spécialement conçue ;
- MS13-070 qui concerne Microsoft OLE, cette mise à jour corrige une vulnérabilité qui pourrait permettre l'exécution de code à distance, si un utilisateur ouvrait un fichier contenant un objet OLE spécialement conçu.

Neuf bulletins sont considérés comme importants, ils concernent :

- une vulnérabilité dans Microsoft Theme File (MS13-071) ;
- des vulnérabilités dans Microsoft Office (MS13-072) ;
- des vulnérabilités dans Microsoft Excel (MS13-073) ;
- des vulnérabilités dans Microsoft Access (MS13-074) ;
- une vulnérabilité dans Microsoft Éditeur IME Microsoft Office (MS13-075) ;
- des vulnérabilités dans Microsoft Pilotes en mode noyau (MS13-076) ;
- une vulnérabilité dans Microsoft Gestionnaire de contrôle des services (MS13-077) ;
- une vulnérabilité dans Microsoft FrontPage (MS13-078) ;
- une vulnérabilité dans Microsoft Active Directory (MS13-079).

À cette date, Microsoft n'a pas constaté de codes d'exploitations pour ces vulnérabilités. En revanche, les détails sur la vulnérabilité CVE-2013-3180 (MS13-067) ont été révélés publiquement et pourraient donc être rapidement massivement exploités.

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

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de septembre 2013 :
  http://technet.microsoft.com/security/bulletin/ms13-sep
- Avis CERTA-2013-AVI-512 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-512/
- Avis CERTA-2013-AVI-513 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-513/
- Avis CERTA-2013-AVI-514 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-514/
- Avis CERTA-2013-AVI-515 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-515/
- Avis CERTA-2013-AVI-516 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-516/
- Avis CERTA-2013-AVI-517 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-517/
- Avis CERTA-2013-AVI-518 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-518/
- Avis CERTA-2013-AVI-519 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-519/
- Avis CERTA-2013-AVI-520 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-520/
- Avis CERTA-2013-AVI-521 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-521/
- Avis CERTA-2013-AVI-522 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-522/
- Avis CERTA-2013-AVI-523 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-523/
- Avis CERTA-2013-AVI-524 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-524/

2 Mise à jour Adobe

Adobea publié trois bulletins de sécurité :

- APSB13-21 qui concerne Adobe Flash Player ;
- APSB13-22 qui concerne Adobe Reader et Acrobat ;
- APSB13-23 qui concerne Adobe Shockwave Player.

Les plus graves pourraient permettre l'exécution de code à distance si un utilisateur affichait une page Web spécialement conçue.

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

Documentation

- Avis CERTA-2013-AVI-509 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-509/
- Avis CERTA-2013-AVI-510 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-510/
- Avis CERTA-2013-AVI-511 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-511/

3 Fin de support de Microsoft Office 2003

De nombreux systèmes utilisant Microsoft Office 2003 sont aujourd'hui encore en service dans les administrations et les entreprises. Microsoft a planifié l'arrêt du support de Microsoft Office 2003 en même temps que Windows XP, c'est à dire le 14 avril 2014. A cette date, l'éditeur cessera d'assurer la publication de correctifs de sécurité, y compris en cas de découverte d'une vulnérabilité critique.

Il est important de souligner que l'arrêt du support de Office 2003 va entraîner une recrudescence des codes d'exploitations de type « 0-day » dans les kits d'exploitation. Les vendeurs de vulnérabilités vont probablement en profiter pour écouler leur réserve de « 0-day » qui auront d'autant plus de valeur pour les attaquants, car les vulnérabilités ne seront plus corrigées par l'éditeur.

Le support et la mise à disposition de mises à jour de sécurité par l'éditeur sont des points cruciaux de la sécurisation d'un serveur ou d'une station de travail. L'arrêt du support d'une version d'application doit être anticipé et constitue une motivation à la migration vers une version récente soutenue.

De plus, la durée de vie des applications bureautiques retenues pour la migration doit être adaptée au cycle de vie des projets et à la vitesse de renouvellement du parc informatique.

Le CERTA attire votre attention sur la nécessité d'anticiper dès à présent une migration vers des applications bureautiques dont la pérennité des mises à jour de sécurité pourra être assurée après cette date.

4 Prévention des risques liés au vol d'ordinateur portable

L'utilisation professionnelle d'ordinateurs portables est aujourd'hui incontournable et concerne la grande majorité des catégories de personnels d'une organisation (de l'employé au dirigeant). Après avoir largement remis en question la sécurité périmétrique des entreprises en raison du passage constant de l'ordinateur portable de l'extérieur du réseau (ADSL personnel, hotspots wifi, hotels, etc.) à l'intérieur, l'emploi d'ordinateurs portables occasionne des risques spécifiques comme la perte ou le vol.

Chaque année des milliers d'ordinateurs portables sont perdus ou volés (taxis, aéroports, hôtels, etc.) impliquant un dommage potentiel bien supérieur à la simple valeur du matériel. En effet, ces ordinateurs conservent localement sur le disque dur un ensemble de données dont la sensibilité est souvent sous-évaluée.

On s'attend bien-sûr à la valeur des documents professionnels, mais d'autres données sensibles de l'entité sont aussi exposées par la perte d'un portable :

- les données de la messagerie (messages reçus et émis, contacts, annuaire, etc.) ;
- les éléments de connexion aux services d'infrastructure :
  - serveurs de messagerie,
  - comptes et mots de passe enregistrés dans le navigateur (applications métiers accédées en extranet, serveur de messagerie OWA, etc.),
  - comptes et mots de passe d'accès au VPN,
  - certificats utilisateur ou machine dont la clé privée est stockée sur le poste nomade,
- les comptes de services, des applications COM+ et des tâches planifiées (utilisateur et mot de passe).

Il est donc important, à minima, d'avoir un inventaire aussi détaillé que possible des identifiants, secrets et informations exposés à la divulgation. Cet inventaire permet notamment d'identifier l'exposition de l'organisation à la divulgation de ces données. Par exemple, si un compte privilégié est compromis, il sera nécessaire d'en changer en urgence le mot de passe. Cette simple opération peut se révéler lourde de conséquences, notamment si ce compte est utilisé sur un grand nombre de machines dans des contextes différents. Une fois l'inventaire réalisé, il conviendra de :

- revoir la politique d'utilisation des comptes pour éliminer ou limiter les expositions inutiles ;
- prendre les mesures de protection des données :
  - mise en place de techniques de chiffrement de volumes (BitLocker, TrueCrypt, FileVault, LUKS, etc.),
  - sensibiliser les utilisateurs sur la bonne gestion des données en mobilité (ne pas accumuler inutilement des milliers de fichiers professionnels),
- mettre en place les mesures de réduction de la surface d'attaque (désactivation protocoles sans fils : Bluetooth, Wifi, etc.),
- privilégier les transferts d'information via un canal sécurisé et journalisé, à un stockage massif de documents sur le disque local.

De plus, une procédure de remédiation de la perte d'un ordinateur portable doit comporter les mesures de :

- changements de mots de passe ;
- révocation de certificats machines/utilisateur ;
- surveillance accrue de l'activité des comptes de l'utilisateur sur la supervision ;
- en cas retour du portable perdu/volé :
  - ne pas reconnecter l'ordinateur au système d'information,
  - si pertinent, confier la machine à un service compétent pour analyse,
  - formater/Réinstaller la machine avant affectation,
- etc.

Enfin, le CERTA rappelle qu'un « Passeport de conseils aux voyageurs », décrivant un ensemble de règles simples pour réduire le risque et les menaces lors du transport de matériel informatique (terminaux mobiles, ordinateurs portables, etc.) est disponible sur le site `http://www.securite-informatique.gouv.fr/partirenmission/`

Documentation

- Passeport de conseils aux voyageurs :
  http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf

5 Rappel des avis émis

Dans la période du 06 au 12 septembre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-505 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-506 : Vulnérabilité dans DNS Response Rate Limiting
- CERTA-2013-AVI-507 : Multiples vulnérabilités dans le noyau Linux de Ubuntu
- CERTA-2013-AVI-508 : Multiples vulnérabilités dans les produits Juniper
- CERTA-2013-AVI-509 : Multiples vulnérabilités dans Adobe Flash Player
- CERTA-2013-AVI-510 : Multiples vulnérabilités dans Adobe Reader et Acrobat
- CERTA-2013-AVI-511 : Multiples vulnérabilités dans Adobe Shockwave Player
- CERTA-2013-AVI-512 : Multiples vulnérabilités dans Microsoft SharePoint Server
- CERTA-2013-AVI-513 : Vulnérabilité dans Microsoft Outlook
- CERTA-2013-AVI-514 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-515 : Vulnérabilité dans Microsoft OLE
- CERTA-2013-AVI-516 : Vulnérabilité dans Microsoft Theme File
- CERTA-2013-AVI-517 : Multiples vulnérabilités dans Microsoft Office
- CERTA-2013-AVI-518 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2013-AVI-519 : Multiples vulnérabilités dans Microsoft Access
- CERTA-2013-AVI-520 : Vulnérabilité dans Microsoft Éditeur IME Microsoft Office (version en chinois)
- CERTA-2013-AVI-521 : Multiples vulnérabilités dans Microsoft Pilotes en mode noyau
- CERTA-2013-AVI-522 : Vulnérabilité dans Microsoft Gestionnaire de contrôle des services
- CERTA-2013-AVI-523 : Vulnérabilité dans Microsoft FrontPage
- CERTA-2013-AVI-524 : Vulnérabilité dans Microsoft Active Directory
- CERTA-2013-AVI-525 : Multiples vulnérabilités dans Wireshark
- CERTA-2013-AVI-526 : Multiples vulnérabilités dans WordPress
- CERTA-2013-AVI-527 : Multiples vulnérabilités dans les produits Juniper

Gestion détaillée du document

13 septembre 2013 version initiale.