Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 décembre 2013
N° CERTA-2013-ACT-051

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-051

1 Publication de bonnes pratiques informatiques pour les collectivités locales

L'ANSSI a publié cette semaine un dépliant listant des bonnes pratiques informatiques à destination des collectivités locales.

Ce dépliant rappelle les différents risques visant ces systèmes d'informations :

- défiguration de sites Web ;
- filoutages par courrier électronique ;
- vol de données ;
- etc.

Il présente également les premières démarches à entreprendre pour réduire ces risques, comme l'application du guide d'hygiène informatique ou le recours à des prestataires de confiance.

Documentation

- Bonnes pratiques informatiques pour les collectivités locales :
  http://www.ssi.gouv.fr/IMG/pdf/sensibilisation_collectivites_locales-ANSSI.pdf

2 Publication d'une note concernant les politiques de restrictions logicielles

L'ANSSI a récemment publié une note technique contenant des recommandations pour la mise en œuvre d'une politique de restrictions logicielles grâce au mécanisme AppLocker de Windows.

Ce mécanisme, disponible à partir de Windows 7 (édition entreprise) et Windows Server 2008, permet de définir des listes blanches de programmes dont l'exécution sera autorisée pour certains utilisateurs en fonction de la politique configurée sur le domaine. Il succède au mécanisme SRP (*Software Restriction Policies*), disponible depuis Windows XP/2003.

La note s'adresse aux administrateurs de parcs Windows ainsi qu'aux responsables informatiques.

Elle reprend les possibilités offertes par AppLocker ainsi que les différents écueils à prendre en compte. Sont notamment abordées la gestion des interpréteurs de scripts, la gestion des bibliothèques dynamiques ou encore l'instanciation des composants ActiveX.

Documentation

- Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows :
  http://www.ssi.gouv.fr/IMG/pdf/NP_Applocker_NoteTech-v1.pdf

3 Vol de jeton d'accès Microsoft Office 365

Lors de sa dernière mise à jour mensuelle, Microsoft a publié le correctif de sécurité MS13-104 pour Microsoft Office. Il corrige la vulnérabilité CVE-2013-5054 dont l'exploitation peut permettre une divulgation d'informations lors de l'ouverture d'un fichier Microsoft Office hébergé sur un site Web malveillant. En effet, la vulnérabilité permet à un attaquant de voler le jeton d'accès d'un utilisateur qui lui permet de s'authentifier à un service d'informatique en nuage Microsoft Office 365 (SharePoint Online, SkyDrive Pro, etc.).

Lorsqu'un utilisateur accède à un document Microsoft Office hébergé sur l'espace SharePoint Online de son organisme (via une URL de type « `http://organisme.sharepoint.com` »), le service a besoin du jeton d'accès fourni par l'application cliente Microsoft Office pour autoriser ou non l'accès. Pour cela, l'application cliente utilise le protocole HTTP ou HTTPS pour envoyer son jeton au service SharePoint afin de récupérer un cookie de session qui lui permettra d'accéder aux documents.

Le protocole simplifié derrière l'envoi de jeton est le suivant :

- le client Microsoft Office (par exemple Word) envoie une requête `HTTP OPTIONS` vers l'URL du dossier contenant le document qu'il souhaite éditer ;
- le service SharePoint répond avec un message `HTTP Response` de type 401 (non autorisé) mais en précisant des informations dans l'entête `WWW-Authenticate` pour poursuivre le processus d'authentification ;
- le client Microsoft Office (Word) utilise alors les informations contenues dans l'entête `WWW-Authenticate` pour envoyer son jeton d'authentification au service *IDCRL* (« IDentity Client Runtime Library service ») de Microsoft Office 365 qui gère l'authentification du client ;
- le service *IDCRL* répond alors avec un message `HTTP RESPONSE` de type 200 (OK) avec dans l'entête `Set-Cookie` le cookie qui permettra d'accéder aux documents.

La vulnérabilité est présente dans la 2e étape du protocole décrit précédemment. En effet, Microsoft Office (par exemple Word) va retourner le jeton d'accès qui correspond au champ `RootDomain` de l'entête `WWW-Authenticate` (par exemple « `sharepoint.com` »), sans vérifier la valeur de ce champ par rapport à l'hôte présent dans l'URL de connexion ou les informations contenues dans le certificat TLS présenté par le service. Il est donc possible de mettre en place un serveur HTTP malveillant qui renvoie dans l'entête `WWW-Authenticate` les champs attendus afin de se faire passer pour un serveur SharePoint légitime et ainsi récupérer le jeton d'authentification du client.

Les attaques observées utilisent le scénario suivant pour accéder aux documents du site SharePoint d'un organisme :

- l'attaquant met en place un site web malveillant (serveur Web) se faisant passer pour le site SharePoint légitime de l'organisme ;
- l'attaquant envoie alors à sa victime un courriel en usurpant l'adresse e-mail d'un collègue de travail avec un lien pointant sur un document Office hébergé sur le site malveillant ;
- la victime, en se connectant sur le lien présent dans le courriel reçu, va alors divulguer à l'attaquant son jeton d'accès.

Cette vulnérabilité est intéressante du point de vue d'un attaquant car elle permet de récupérer facilement le jeton d'authentification d'un client à l'aide d'un site web spécialement conçu et d'accéder ensuite au service SharePoint utilisé par le client.

Le CERTA recommande l'application du correctif Microsoft dès que possible et également d'être vigilant lors de la réception de courriels contenant des liens vers des documents hébergés sur des services SharePoint.

Documentation

- Bulletin de sécurité Microsoft MS13-104 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-104
- Severe Office 365 Token Disclosure Vulnerability :
  http://www.adallom.com/blog/severe-office-365-token-disclosure-vulnerability-research-and-analysis/

4 Rappel des avis émis

Dans la période du 13 au 19 décembre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-675 : Multiples vulnérabilités dans TYPO3 CMS
- CERTA-2013-AVI-676 : Multiples vulnérabilités dans les systèmes SCADA Siemens
- CERTA-2013-AVI-677 : Multiples vulnérabilités dans Apple Safari
- CERTA-2013-AVI-678 : Vulnérabilité dans Apple OS X Mavericks
- CERTA-2013-AVI-679 : Multiples vulnérabilités dans Wireshark
- CERTA-2013-AVI-680 : Multiples vulnérabilités dans Asterisk
- CERTA-2013-AVI-681 : Vulnérabilité dans Puppet

Gestion détaillée du document

20 décembre 2013 version initiale.