Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 11 octobre 2013
N° CERTA-2013-ACT-041

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-041

1 - Mise à jour mensuelle Microsoft

Lors de sa dernière mise à jour mensuelle, Microsoft a publié huit bulletins de sécurité. Les quatre bulletins suivants sont considérés comme critiques :

- MS13-080 qui concerne Internet Explorer, cette mise à jour corrige dix vulnérabilités ;
- MS13-081 qui concerne les pilotes en mode noyau de Windows, cette mise à jour corrige sept vulnérabilités ;
- MS13-082 qui concerne .NET Framework, cette mise à jour corrige deux vulnérabilités ;
- MS13-083 qui concerne la bibliothèque de contrôles communs de Windows, cette mise à jour corrige une vulnérabilité.

Les vulnérabilités corrigées dans les correctif MS13-080 à MS13-83 pourraient, pour les plus dangereuses, permettre l'exécution de code à distance.

Le correctif MS13-080 corrige la vulnérabilité activement exploitée et évoquée dans l'alerte CERTA-2013-ALE-006. Cette mise à jour ferme donc l'alerte de sécurité.

Les quatre bulletins suivants sont considérés comme importants :

- MS13-084 qui concerne SharePoint Server, cette mise à jour corrige deux vulnérabilités ;
- MS13-085 qui concerne Microsoft Excel, cette mise à jour corrige deux vulnérabilités ;
- MS13-086 qui concerne Microsoft Word, cette mise à jour corrige deux vulnérabilités ;
- MS13-087 qui concerne Microsoft Silverlight, cette mise à jour corrige une vulnérabilité qui pourrait permettre une divulgation d'informations.

Les vulnérabilités corrigées dans les correctifs MS13-084 à MS13-86 pourraient permettre l'exécution de code à distance.

Le CERTA recommande l'application de ces mises à jour dès que possible.

Documentation

- Synthèse des bulletins de sécurité Microsoft du mois de août 2013 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms13-oct
- Bulletin d'alerte portant sur une vulnérabilité dans Microsoft internet explorer :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-ALE-006/index.html
- Avis du CERTA portant sur les bulletins de sécurité de Microsoft :
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-559/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-560/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-561/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-562/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-563/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-564/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-565/index.html
  http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-566/index.html

2 - Mise à jour Adobe

Adobe a publié deux bulletins de sécurité :

– APSB13-24 qui concerne Adobe RoboHelp ;

– APSB13-25 qui concerne Adobe Reader et Acrobat.

La première vulnérabilité pourrait permettre l'exécution de code arbitraire au moyen d'une altération des données en mémoire. La seconde permettrait de contourner des contrôles de sécurités concernant l'exécution de codes javascript.

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

Documentation

– Avis CERTA-2013-AVI-577 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-557/index.html

– Avis CERTA-2013-AVI-578 :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-558/index.html

3 - Sécurité des composants bas niveau du système

3 -.1 BIOS et UEFI

Jusqu'à récemment, le niveau de privilèges le plus élevé visé par les attaquants était l'exécution de code en mode noyau, qui permet la prise de contrôle de l'intégralité du système d'exploitation. Mais le renforcement des mécanismes de sécurité pousse les attaquants à obtenir une persistance à plus bas niveau, c'est-à-dire plus proche du matériel.

Une présentation à la conférence Ekoparty, en septembre, a justement exposé certains risques liés aux BIOS et UEFI : la possibilité pour un attaquant d'insérer du code malveillant dans ces éléments critiques pour la sécurité du système, car exécutés dès le démarrage de la machine.

Après avoir rappellé que l'activation de la vérification de signature pour la mise à jour du BIOS est un strict minimum, les chercheurs ont présenté deux attaques permettant de contourner la vérification de la signature lors de la mise à jour du BIOS. Ils ont ainsi pu exécuter du code arbitraire avec le plus haut niveau de privilèges et prendre le contrôle complet de la machine.

3 -.2 Micrologiciels et microcodes

Le BIOS n'est pas le seul moyen pour les attaquants de garder le contrôle en dehors du système d'exploitation. Certains périphériques disposent de leur propre code pour leur gestion interne. Par exemple, les cartes réseau ou les cartes RAID embarquent généralement un processeur dédié. Comme tous les autres, ces codes peuvent présenter des vulnérabilités, éventuellement exploitables par un attaquant, qui pourra alors profiter des accès privilégiés des périphériques à la mémoire du système ou encore insérer du code exécuté à l'initialisation de la machine.

De la même manière, le processeur lui-même peut présenter des vulnérabilités. Il est parfois possible de les corriger en mettant à jour le processeur avec un *microcode*. Ces mises à jour sont généralement fournies par les éditeurs de BIOS, qui se charge alors de mettre à jour le processeur au démarrage. La plupart des distributions Linux proposent également des paquets offrant la même fonctionnalité.

Le CERTA recommande donc de porter attention aux mises à jour fournies par les constructeurs de tous les matériels utilisés sur le parc et de mettre à jour les différents micrologiciels et microcodes lorsque nécessaire. Une qualification de ces mises à jour est fortement recommandée, car d'éventuels problèmes pourraient entraîner un dysfonctionnement complet du matériel.

Documentation

– Vulnérabilité dans Dell Latitude et Precision :
http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-567/

4 - Code malveillant Shiotob

Cette semaine, le Malware Protection Center de Microsoft a communiqué des éléments sur la famille de codes malveillants `Win32/Shiotob`. Cette famille a été vue pour la première fois en 2011. Elle permet de voler les informations systèmes et personnelles de la victime en surveillant le trafic réseau.

`Shiotob` est activement et massivement utilisé par des cyber-criminels. A ce titre, le CERTA rediffuse les éléments communiqués publiquement par Microsoft pour identifier ce code malveillant.

`Shiotob` se répand en envoyant des mails aux victimes avec le code malveillant en pièce jointe. Il dispose d'une fonctionnalité lui permettant de récupérer les adresses mails sur les machines infectées.

Voici des exemples de noms de pièces jointes :

- `DHL_Express_POST-NOTIFICATION_<chaine aléatoire>.zip`
- `Booking_Hotel_Reservation_Details_<chaine aléatoire>.zip`
- `DHL-International-Delivery-Notification_<chaine aléatoire>.zip`
- `DHL_ONLINE_SHIPPING_PREALERT_<chaine aléatoire>.zip`
- `DHL-Worldwide-Delivery-Notification-<chaine aléatoire>.zip`

Pour masquer sa présence du gestionnaire de tâche de Microsoft Windows, ce troyen injecte son code malveillant dans des processus légitimes du système d'exploitation : `csrss.exe`, `svchost.exe`, `iexplore.exe`, `explore.exe`.

`Shiotob` utilise deux moyens de persistance à l'aide de la base de registre. La première méthode est l'ajout d'une valeur dans la sous-clef Run de la base de registre :

- sous-clé de registre : `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`
- valeur : nom aléatoire
- contenu de la valeur : `<chemin du code malveillant> -autorun`

La deuxième méthode, un peu plus originale, est la définition du code malveillant en tant que "Debugger" pour le programme "userinit.exe" au niveau de la sous-clé "Image File Execution Options" de la base de registre :

- sous-clé de registre : `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\userinit.exe`
- valeur : `Debugger`
- contenu de la valeur : `<chemin du code malveillant>`

Cette méthode permet de lancer automatiquement le code malveillant lorsque le programme `userinit.exe` est lancé pendant la phase d'ouverture de session de l'utilisateur.

De plus, le programme malveillant envoie les informations volées à l'aide de requêtes HTTP POST. Il s'injecte aussi dans de nombreux processus, principalement des navigateurs web, des clients mail et des clients FTP. Pour récupérer les informations de la victime dans ces applications, `Shiotob` détourne le flux d'exécution des principales fonctions de l'API Windows vers son code malveillant. Les fonctions détournées sont majoritairement celles utilisées pour envoyer et recevoir des données sur le réseau : `Closesocket`, `Connect`, `HttpOpenRequestA`, `HttpOpenRequestW`, `HttpQueryInfoA`, `HttpQueryInfoW`, `HttpSendRequestA`, `HttpSendRequestW`, `InternetCloseHandle`, `InternetQueryDataAvailable`, `InternetReadFile`, `InternetReadFileExA`, `InternetWriteFileExW`, `Send`.

Enfin, un dernier marqueur d'infection du code malveillant est l'utilisation d'une sous-clé de registre aléatoire dans la partie des paramètres Internet de la base de registre pour stocker des informations chiffrées de l'utilisateur avant d'être exfiltrées :

- sous-clé de registre : `HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\<numéro de version>\<chaîne aléatoire>`
- valeur : `(default)`
- contenu de la valeur : `<informations chiffrées>`

Le CERTA recommande de vérifier que les marqueurs ne sont pas présents sur votre parc et de se référer à la note d'information du CERTA "Les bons réflexes en cas d'intrusion sur un système d'information" en cas de suspicion de compromission.

Documentation

- MSRT October 2013 - Shiotob
  http://blogs.technet.com/b/mmpc/archive/2013/10/08/msrt-october-2013-shiotob.aspx
- Les bons réflexes en cas d'intrusion sur un système d'information
  http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002/index.html

5 - Rappel des avis émis

Dans la période du 04 au 10 octobre 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-554 : Vulnérabilité dans Apple OS X Mountain Lion
- CERTA-2013-AVI-555 : Vulnérabilité dans EMC Atmos
- CERTA-2013-AVI-556 : Vulnérabilité dans GnuPG
- CERTA-2013-AVI-557 : Vulnérabilité dans Adobe RoboHelp
- CERTA-2013-AVI-558 : Vulnérabilité dans Adobe Reader et Acrobat
- CERTA-2013-AVI-559 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTA-2013-AVI-560 : Multiples vulnérabilités dans Microsoft Windows Kernel-Mode Drivers
- CERTA-2013-AVI-561 : Multiples vulnérabilités dans Microsoft .NET Framework
- CERTA-2013-AVI-562 : Vulnérabilité dans Microsoft Windows Common Control Library
- CERTA-2013-AVI-563 : Multiples vulnérabilités dans Microsoft SharePoint Server
- CERTA-2013-AVI-564 : Multiples vulnérabilités dans Microsoft Excel
- CERTA-2013-AVI-565 : Multiples vulnérabilités dans Microsoft Office
- CERTA-2013-AVI-566 : Vulnérabilité dans Microsoft Silverlight
- CERTA-2013-AVI-567 : Vulnérabilité dans Dell Latitude et Precision
- CERTA-2013-AVI-568 : Multiples vulnérabilités dans Cisco Cisco Firewall Services Module
- CERTA-2013-AVI-569 : Multiples vulnérabilités dans Cisco ASA Software

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

- CERTA-2013-ALE-006-001 : Vulnérabilité dans Microsoft Internet Explorer (fermeture de l'alerte, suite à la diffusion du correctif par l'éditeur.)

Gestion détaillée du document

11 octobre 2013 version initiale.