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 14 septembre 2015
N° CERTFR-2015-ACT-037

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-037

1 - Fichiers Adobe flash dans les documents Microsoft Office

Introduction

De précédents bulletins d'actualités ont évoqué les dangers liés à l'exécution automatique de contenu dynamique, comme Adobe Flash, par un navigateur Internet.

Les nombreuses vulnérabilités rencontrées par ce format poussent les éditeurs des navigateurs à privilégier des solutions alternatives afin de préserver la sécurité de leurs utilisateurs et augmenter par ailleurs la durée de vie des batteries d'ordiphones, tablettes et autres ordinateurs nomades. Ainsi, dans sa dernière version, Google Chrome suspend automatiquement la lecture des modules Flash considérés comme secondaires présents sur une page web (généralement les publicités), laissant le choix à l'utilisateur d'exécuter ou non ce contenu via un simple clic.

Pour les autres navigateurs, l'utilisateur doit avoir recours à des greffons (de type click-to-play) lui permettant de configurer le mode d'exécution (automatique ou suspendu) des contenus dynamiques. Malheureusement, ces solutions ne peuvent procurer à l'utilisateur qu'un contrôle partiel. En effet, ces vulnérabilités Flash, telles que CVE-2015-5122 peuvent aussi être exploitées au sein de documents numériques (Office ou Adobe Acrobat, PDF), souvent transmis en pièce jointe ou via une clé USB.

L'exécution des contenus Flash peut être explicitement désactivée dans Microsoft Office ainsi que dans Adobe Reader.

Document office

La fonctionnalité de bit d'arrêt documentée dans l'alerte de sécurité Microsoft 27558014 permet de désactiver l'exécution des contenus Flash dans les documents Office.

1. Créer un fichier texte Disable_flash.reg avec le contenu suivant :

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\Common\COM\Compatibility\{D27CDB6E-AE6
"Compatibility Flags"=dword:00000400
```

2. Dans l'éditeur de base de registre, importer ce fichier .reg

Ce paramétrage peut aussi être déployé dans un parc informatique à travers un objet de stratégie de groupe (GPO) ou toute autre solution de déploiement à votre disposition.

Adobe Acrobat

Par défaut, les versions récentes d'Adobe Acrobat Reader activent le mode protégé. Dans ce mode, le lecteur de document bloque l'exécution de fichiers exécutables arbitraires depuis les répertoires du système ou la base de registre Windows. Ainsi, lors de l'ouverture d'un document PDF malveillant, les exécutions non désirées sont suspendues par défaut (l'utilisateur conserve la possibilité d'activer manuellement ces exécutions).

Pour vérifier la configuration du mode protégé, il est possible de visualiser les paramètres via les menus Fichier >Propriétés >Avancés >Mode Protégé.

Cependant, si les contenus Flash ne sont pas jugés nécessaires à l'exploitation des documents professionnels de l'entité, il est recommandé de les désactiver explicitement au moyen de la valeur de la base de registre suivante :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\<product>\<Version>\FeatureLockDown]
"bEnableFlash" = DWORD:0
```

Recommendations

Ces mesures de protection spécifiques ne sauraient se substituer aux bonnes pratiques liées à l'utilisation de la messagerie électronique, notamment les points relatifs à l'ouverture des pièces jointes, à savoir:

- s'assurer que le message provient d'un contact connu ;
- si le message (ou sa pièce jointe) n'est pas attendu, s'assurer de la pertinence du message avant de l'ouvrir. Dans le doute, il est pertinent de s'assurer de la légitimité du message auprès de son émetteur ;
- si un comportement inhabituel est observé par l'utilisateur lors de l'ouverture du message, il convient de prévenir la hiérarchie ou directement le responsable de la sécurité informatique ;

D'une façon plus générale, l'ANSSI recommande de maintenir en condition de sécurité le poste utilisé pour la lecture de messages électroniques :

- utiliser un antivirus et le maintenir à jour ;
- maintenir à jour le système d'exploitation et les différentes applications ;
- bloquer ou désactiver les fonctionnalités non utilisées.

Le CERT-FR conseille également d'installer des outils permettant de durcir les systèmes et de rendre l'exploitation de vulnérabilités plus difficile. Sous Microsoft Windows, l'outil EMET proposé par Microsoft, permet de bloquer l'exploitation de vulnérabilités, en particulier la CVE-2015-5122.

Documentation

- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-009/CERTFR-2014-ACT-009.html
- http://blog.fortinet.com/post/you-disabled-flash-in-your-browsers-but-is-that-enough
- http://blogs.technet.com/b/srd/archive/2008/02/06/the-kill_2d00_bit-faq_3a00_-part-1-of-3.aspx
- https://technet.microsoft.com/en-us/library/security/2755801.aspx
- http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-010/CERTFR-2014-ACT-010.html

2 - Mise à jour mensuelle de Microsoft

Le 8 septembre 2015, Microsoft a publié 12 bulletins de sécurité, dont 5 sont considérés comme critiques et 7 comme importants :

- MS15-095 (critique) qui concerne Microsoft Edge ;
- MS15-097 (critique) qui concerne le composant graphique de Windows ;
- MS15-098 (critique) qui concerne le journal Windows ;
- MS15-099 (critique) qui concerne Microsoft Office ;
- MS15-094 (critique) qui concerne Internet Explorer ;
- MS15-096 (important) qui concerne le service Active Directory de Windows ;
- MS15-100 (important) qui concerne le centre de divertissement de Windows ;
- MS15-101 (important) qui concerne le cadre de travail .NET ;
- MS15-102 (important) qui concerne la gestion des tâches de Windows ;
- MS15-103 (important) qui concerne le serveur Exchange de Windows ;
- MS15-104 (important) qui concerne les serveurs Skype entreprise et Lync ;
- MS15-105 (important) qui concerne l'hyperviseur Hyper-V.

Quatre vulnérabilités critiques ont été corrigées au sein du navigateur Microsoft Edge de Windows 10. Elles concernent des corruptions de la mémoire et permettent d'exécuter du code arbitraire à distance. Microsoft indique qu'une d'entre elles a été révélée publiquement, sans être exploitée.

Une vulnérabilité a été corrigée dans le service Active Directory de Windows serveur. Elle pourrait mener à un déni de service à distance. Pour exploiter cette vulnérabilité, un attaquant doit posséder un compte doté de privilèges autorisant la jonction d'ordinateurs au domaine.

Le bulletin MS15-097 fait état de onze vulnérabilités dans le composant graphique de Windows. Quatre d'entre elles concernent le pilote lié au traitement des polices, les autres sont des corruptions mémoire dans Win32k. La vulnérabilité identifiée par la référence CVE-2015-2546 a été exploitée publiquement, elle permet une élévation de privilèges.

Le journal Windows a fait l'objet de cinq corrections. Ces vulnérabilités sont critiques, elles permettent d'exécuter du code arbitraire à distance lors de l'ouverture d'un fichier du journal Windows.

Plusieurs vulnérabilités ont été corrigées dans les serveurs Skype entreprise et Lync de Windows. Ces vulnérabilités sont des injections de script inter-sites qui pourraient entraîner une élévation de privilèges.

Les versions Windows et Mac de Microsoft Office ont été mises à jour afin de corriger quatre vulnérabilités liées à une corruption mémoire. Aucune n'a été révélée publiquement.
Une vulnérabilité permettant une exécution de code à distance a été corrigée dans le centre de divertissement Windows. La vulnérabilité peut se déclencher si l'utilisateur ouvre un fichier de liaison Media Center (.mcl).

Le cadriciel .NET a été mis à jour afin de corriger deux vulnérabilités qui permettent une élévation de privilèges et un déni de service. La première concerne la manière dont la validation du nombre d'objets en mémoire est effectuée, avant de les copier dans un bloc.

Trois vulnérabilités ont fait l'objet d'une correction dans la gestion des tâches de Windows, elles affectent toutes les versions de Windows depuis Windows Vista et permettent une élévation locale de privilèges.

Le serveur Microsoft Exchange de Windows a été mis à jour suite à la découverte de trois vulnérabilités qui pourraient entraîner une divulgation d'informations ou une usurpation d'identité.

Une vulnérabilité a été corrigée dans l'hyperviseur Hyper-V, elle pourrait permettre de contourner certaines mesures de sécurité liées au contrôle d'accès par liste ACL.

Enfin, 17 vulnérabilités ont été corrigées au sein du navigateur Internet Explorer. Elles concernent des corruptions de la mémoire, certaines pouvant mener à une exécution de code arbitraire à distance. Ces vulnérabilités touchent toutes les versions du navigateur, depuis la version 7 jusqu'à la version 11. Aucune de ces vulnérabilités n'a été exploitée publiquement.

Le CERT-FR rappelle l'importance de ces correctifs de sécurité et recommande de les appliquer dès que possible.

Documentation

- https://technet.microsoft.com/library/security/MS15-094
- https://technet.microsoft.com/library/security/MS15-095
- https://technet.microsoft.com/library/security/MS15-096
- https://technet.microsoft.com/library/security/MS15-097
- https://technet.microsoft.com/library/security/MS15-098
- https://technet.microsoft.com/library/security/MS15-099
- https://technet.microsoft.com/library/security/MS15-100
- https://technet.microsoft.com/library/security/MS15-101
- https://technet.microsoft.com/library/security/MS15-102
- https://technet.microsoft.com/library/security/MS15-103
- https://technet.microsoft.com/library/security/MS15-104
- https://technet.microsoft.com/library/security/MS15-105

3 - Rappel des avis émis

Dans la période du 07 au 13 septembre 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-370 : Multiples vulnérabilités dans MediaWiki
- CERTFR-2015-AVI-371 : Multiples vulnérabilités dans les produits Mozilla
- CERTFR-2015-AVI-372 : Vulnérabilité dans le noyau Linux Ubuntu
- CERTFR-2015-AVI-373 : Vulnérabilité dans Microsoft Windows Media Center
- CERTFR-2015-AVI-374 : Multiples vulnérabilités dans Microsoft .NET Framework
- CERTFR-2015-AVI-375 : Multiples vulnérabilités dans le gestionnaire des tâches de Windows
- CERTFR-2015-AVI-376 : Multiples vulnérabilités dans Microsoft Exchange
- CERTFR-2015-AVI-377 : Multiples vulnérabilités dans Microsoft Skype
- CERTFR-2015-AVI-378 : Multiples vulnérabilités dans Microsoft Hyper-V
- CERTFR-2015-AVI-379 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2015-AVI-380 : Multiples vulnérabilités dans le composant graphique de Microsoft
- CERTFR-2015-AVI-381 : Vulnérabilité dans Microsoft Active Directory
- CERTFR-2015-AVI-382 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2015-AVI-383 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-384 : Multiples vulnérabilités dans Microsoft Windows Journal
- CERTFR-2015-AVI-385 : Multiples vulnérabilités dans les produits Huawei U1900
- CERTFR-2015-AVI-386 : Vulnérabilité dans les produits Huawei WLAN AC
- CERTFR-2015-AVI-387 : Multiples vulnérabilités dans PHP

Gestion détaillée du document

14 septembre 2015 version initiale.