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 15 décembre 2014
N° CERTFR-2014-ACT-050

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-050

1 - Mise à jour mensuelle de Microsoft

Le 9 décembre 2014, Microsoft a publié 7 bulletins de sécurité, dont 3 sont considérés comme critiques et 4 comme importants :

- MS14-075 (important) qui concerne Microsoft Exchange Server ;
- MS14-080 (critique) qui concerne Internet Explorer ;
- MS14-081 (critique) qui concerne Microsoft Word et Microsoft Office Web Apps ;
- MS14-082 (important) qui concerne Microsoft Office ;
- MS14-083 (important) qui concerne Microsoft Excel ;
- MS14-084 (critique) qui concerne le moteur de script VBScript ;
- MS14-085 (important) qui concerne le composant graphique de Microsoft Windows.

Quatre vulnérabilités ont été corrigées dans Microsoft Exchange Server, deux d'entre elles permettent une exécution de code arbitraire à distance si l'attaquant arrive à convaincre l'utilisateur de visiter une page Internet et de cliquer sur un lien spécialement conçu pour exploiter la vulnérabilité.

Internet Explorer fait l'objet de 14 vulnérabilités corrigées. Neuf d'entre elles peuvent être exploitées sur la dernière version du navigateur et douze permettent d'exécuter du code arbitraire à distance. Une corruption mémoire, décrite par la vulnérabilité CVE-2014-6374, permet une exécution de code arbitraire à distance sur l'ensemble des versions du navigateur, d'Internet Explorer 6 à 11. Les autres vulnérabilités peuvent amener à un contournement de certains filtres XSS et de la mesure de sécurité consistant à distribuer de manière aléatoire l'espace d'adressage (ASLR).

Deux vulnérabilités ont été corrigées dans Microsoft Word, elles affectent également Microsoft Office Web Apps et permettent d'exécuter du code arbitraire à distance si l'attaquant parvient à convaincre sa victime d'ouvrir un document Word malveillant.

La vulnérabilité corrigée dans Microsoft Office permet une exécution de code arbitraire à distance avec les mêmes droits que l'utilisateur courant si un ficher malveillant est ouvert.

Le bulletin MS14-083 fait état de deux vulnérabilités dans Microsoft Excel. Une d'entre elles concerne un pointeur invalide et permet d'exécuter du code arbitraire sur toutes les versions de Microsoft Excel, de 2007 à 2013. L'autre vulnérabilité est due à un problème de libération mémoire et permet également d'exécuter du code arbitraire à distance.

Une vulnérabilité a été corrigée dans le moteur de script VBScript, elle peut être déclenchée si l'utilisateur visite une page Internet spécialement conçue. Cette vulnérabilité permet d'exécuter du code arbitraire à distance, dans le contexte de l'utilisateur courant.

Enfin, la dernière vulnérabilité corrigée se trouve dans le composant graphique permettant d'afficher les images JPEG de Microsoft Windows. L'exploitation de cette vulnérabilité permet une fuite d'informations pouvant par exemple permettre de contourner des mesures de sécurité telle que la distribution aléatoire de l'espace d'adressage (ASLR).

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/ms14-075
- https://technet.microsoft.com/library/security/ms14-080
- https://technet.microsoft.com/library/security/ms14-081
- https://technet.microsoft.com/library/security/ms14-082
- https://technet.microsoft.com/library/security/ms14-083
- https://technet.microsoft.com/library/security/ms14-084
- https://technet.microsoft.com/library/security/ms14-085

2 - Visite d'un intervenant

Les organismes ou entités reçoivent souvent dans leurs locaux des intervenants externes à des fins de démonstration ou de présentation.

Les supports externes apportés par ces visiteurs (disque ou clé USB pour ne nommer que ces deux éléments) peuvent être vecteurs de code malveillant, bien souvent à l'insu du visiteur.

Le CERT-FR renouvelle ses recommandations concernant les périphériques amovibles, parmi lesquelles :

- adopter des pratiques compatibles avec la politique de sécurité de l'entité ou la réglementation (environnement classifié) ;
- ne pas connecter un support extérieur à un poste de l'entité susceptible de contenir des informations sensibles, et à plus forte raison si celui-ci est relié au réseau interne. Une pratique courante consiste à dédier et isoler le matériel utilisé dans le cadre d'une présentation.

Documentation

- http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

3 - Rappel des avis émis

Dans la période du 08 au 14 décembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-507 : Multiples vulnérabilités dans VMware
- CERTFR-2014-AVI-508 : Multiples vulnérabilités dans MediaWiki
- CERTFR-2014-AVI-509 : Multiples vulnérabilités dans les produits IBM
- CERTFR-2014-AVI-510 : Vulnérabilité dans Citrix CloudPlatform
- CERTFR-2014-AVI-511 : Vulnérabilité dans Cisco Unified Computing System Manager
- CERTFR-2014-AVI-512 : Multiples vulnérabilités dans plusieurs produits DNS
- CERTFR-2014-AVI-513 : Multiples vulnérabilités dans les produits IBM
- CERTFR-2014-AVI-514 : Vulnérabilité dans Cisco Unified Communications Domain Manager
- CERTFR-2014-AVI-515 : Vulnérabilité dans Microsoft VBScript Scripting Engine
- CERTFR-2014-AVI-516 : Vulnérabilité dans le composant graphique de Microsoft Windows
- CERTFR-2014-AVI-517 : Multiples vulnérabilités dans Microsoft Exchange Server Could
- CERTFR-2014-AVI-518 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2014-AVI-519 : Multiples vulnérabilités dans Microsoft Word et Microsoft Office Web Apps
- CERTFR-2014-AVI-520 : Vulnérabilité dans Microsoft Office
- CERTFR-2014-AVI-521 : Multiples vulnérabilités dans Microsoft Excel
- CERTFR-2014-AVI-522 : Multiples vulnérabilités dans Adobe Flash
- CERTFR-2014-AVI-523 : Multiples vulnérabilités dans Adobe Reader
- CERTFR-2014-AVI-524 : Vulnérabilité dans VMware vCloud Automation Center
- CERTFR-2014-AVI-525 : Multiples vulnérabilités dans les produits IBM
- CERTFR-2014-AVI-526 : Vulnérabilité dans les produits Cisco
- CERTFR-2014-AVI-527 : Vulnérabilité dans TYPO3
- CERTFR-2014-AVI-528 : Multiples vulnérabilités dans le noyau Linux

Gestion détaillée du document

15 décembre 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-050`