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 16 mars 2015
N° CERTFR-2015-ACT-011

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2015-ACT-011

1 - Mise à jour mensuelle de Microsoft

Le 10 mars 2015, Microsoft a publié 14 bulletins de sécurité, dont 5 sont considérés comme critiques et 9 comme importants :

- MS15-018 (critique) qui concerne Internet Explorer ;
- MS15-019 (critique) qui concerne le moteur de script VBScript ;
- MS15-020 (critique) qui concerne Microsoft Windows ;
- MS15-021 (critique) qui concerne le pilote de gestion des polices Adobe ;
- MS15-023 (important) qui concerne un pilote noyau de Windows ;
- MS15-024 (important) qui concerne le composant d'affichage des images PNG ;
- MS15-025 (important) qui concerne le noyau de Windows ;
- MS15-027 (important) qui concerne NETLOGON ;
- MS15-028 (important) qui concerne le gestionnaire des tâches ;
- MS15-029 (important) qui concerne le traitement des images JPEG XR de Windows ;
- MS15-030 (important) qui concerne le protocole de bureau à distance RDP ;
- MS15-031 (important) qui concerne la vulnérabilité FREAK ;
- MS15-022 (critique) qui concerne Microsoft Office ;
- MS15-026 (important) qui concerne Microsoft Exchange Server.

Internet Explorer

Douze vulnérabilités ont été corrigées au sein de Internet Explorer (bulletin MS15-018). Dix d'entre elles sont exploitables sur la dernière version du navigateur, dont huit qui permettent d'exécuter du code arbitraire à distance. Deux corruptions mémoire, identifiées par les vulnérabilités CVE-2015-1625 et CVE-2015-1634, permettent une exécution de code arbitraire à distance sur l'ensemble des versions du navigateur, d'Internet Explorer 6 à 11. Des attaques ont pu être observées pour 5 de ces vulnérabilités. Les deux autres vulnérabilités permettent une élévation de privilèges.

Le moteur de script VBScript fait l'objet d'une correction. La vulnérabilité permet une exécution de code arbitraire à distance via la visite d'une page Internet.

Windows

Le bulletin MS15-020 fait état de deux vulnérabilités dans Microsoft Windows.

Une d'entre elles (vulnérabilité CVE-2015-0081) concerne les services de texte Windows (Windows Text Services), elle permet une exécution de code arbitraire à distance dans le contexte de sécurité de l'utilisateur actif.

L'autre vulnérabilité est due à un problème lors du chargement des bibliothèques de liens dynamiques (DLL) associé au fonctionnement de prévisualisation des icônes. Elle permet également d'exécuter du code lorsque l'utilisateur visite un site Internet, un partage réseau ou un dossier local avec Windows Explorer.

Dans un article sur son blog, HP informe que cette vulnérabilité est un reliquat de celle exploitée par Stuxnet et corrigée en 2010 (CVE-2010-2772, voir documentation).

Le bulletin MS15-021 fait état de huit vulnérabilités corrigées dans le pilote Windows de gestion des polices de caractères. Toutes ces vulnérabilités sont critiques et permettent d'exécuter du code arbitraire à distance avec les privilèges du noyau (anneau zéro).

Quatre vulnérabilités ont été corrigées dans le composant noyau Win32k (buletin MS15-023), une d'entre elles permet une élévation de privilèges et les trois autres une divulgation du contenu de la mémoire noyau. Deux vulnérabilités ont été identifiées au sein du noyau de Windows, elles permettent une élévation locale de privilèges. (bulletin MS15-025)

Le bulletin MS15-024 concerne une vulnérabilité dans la gestion des images au format PNG. Elle peut être exploitée à distance, par exemple si l'utilisateur visite une page Internet contenant une telle image. Cette vulnérabilité permet d'accéder à une partie de la mémoire, en lecture.

NETLOGON a fait l'objet d'une correction (bulletin MS15-027), la vulnérabilité permet d'usurper l'identité d'une machine. Pour être exploitée, l'attaquant doit se trouver sur le réseau de la victime.

Une vulnérabilité a été corrigée dans le gestionnaire des tâches de Windows (bulletin MS15-028), elle permet à un utilisateur d'exécuter des programmes, pour lesquels il n'a pas les droits d'exécution.

Le composant chargé d'afficher les images au format JPEG XR a fait l'objet d'un correctif (bulletin MS15-029). La vulnérabilité est liée à la manipulation d'une partie de la mémoire non initialisée. Cette vulnérabilité entraine une divulgation de certaines informations dans la mémoire.

Le bulletin MS15-030 concerne le protocole de bureau à distance (RDP). Celui-ci est vulnérable à un déni de service dû à une mauvaise libération de la mémoire.

Enfin, la dernière vulnérabilité corrigée concerne la vulnérabilité FREAK (bulletin MS15-031, CVE-2015-0204) présente dans le composant Schannel de Windows. Elle permet de rétrograder la taille des clés RSA. Pour être exploitée, l'attaquant doit au préalable avoir mené une attaque de type « homme au milieu ».

Microsoft Office

Microsoft Office a fait l'objet de cinq corrections (bulletin MS15-022). Seule la vulnérabilité CVE-2015-0086 est critique. Elle concerne les fichiers au format texte riche (rich text) et permet d'exécuter du code arbitraire à distance.

Microsoft Exchange

Cinq vulnérabilités ont été corrigées dans Microsoft Exchange Server (bulletin MS15-026), quatre permettent une élévation de privilèges et la dernière permet à un attaquant de modifier ou d'ajouter des rendez-vous dans l'agenda de tierces personnes.

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/MS15-018
- https://technet.microsoft.com/library/security/MS15-019
- https://technet.microsoft.com/library/security/MS15-020
- https://technet.microsoft.com/library/security/MS15-021
- https://technet.microsoft.com/library/security/MS15-022
- https://technet.microsoft.com/library/security/MS15-023
- https://technet.microsoft.com/library/security/MS15-024
- https://technet.microsoft.com/library/security/MS15-025
- https://technet.microsoft.com/library/security/MS15-026
- https://technet.microsoft.com/library/security/MS15-027
- https://technet.microsoft.com/library/security/MS15-028

- https://technet.microsoft.com/library/security/MS15-029
- https://technet.microsoft.com/library/security/MS15-030
- https://technet.microsoft.com/library/security/MS15-031
- http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/CVE-2015-0096-issue-patched-today-involves-failed-Stuxnet-fix/ba-p/6718402

2 - Chargement USB en libre-service

L'interface USB fait depuis longtemps l'objet d'une attention particulière à cause des risques d'exposition des périphériques et des postes de travail. La généralisation de cette interface en fait une cible privilégiée :

- infection du poste de travail via un périphérique de stockage de source inconnue ;
- infection du périphérique de stockage via un branchement sur un poste non maîtrisé ;
- compromission d'informations potentiellement sensibles en cas de perte ou de vol ;
- piégeage matériel via un micrologiciel modifié ;
- piégeage matériel via un chargeur USB offert en cadeau ;
- etc.

Afin de faciliter le rechargement d'un ordiphone ou d'une tablette qui possède une durée de vie limitée, il est aujourd'hui possible de trouver des bornes dans les gares ferroviaires, les aéroports, les centres commerciaux, abribus, taxis, hôtels, cybercafés, etc.

Ces initiatives ne sont pas exemptes de risques contre le vol d'informations ou la compromission de périphériques. En général les bornes de rechargement se présentent sous la forme d'un port USB femelle (connecteur de type A) ou d'un câble mâle (connecteurs de type Micro-B, Lightning ou 30 broches spécifiques aux produits de marque Apple) dont l'autre extrémité n'est pas visible.

Des solutions physiques existent afin de bloquer toutes transmissions de données via le protocole USB (câble dont les broches utilisées pour l'échange de données ne sont pas connectées).

D'une manière générale, le CERT-FR recommande de ne pas brancher son téléphone professionnel via USB sur un équipement non maîtrisé. La solution la plus simple consiste à utiliser un adaptateur secteur et le cable fournit par le constructeur, branché sur une prise électrique 220 Volts.

Documentation

- Bulletin d'actualité CERTFR-2014-ACT-043 :
  http://www.cert.ssi.gouv.fr/site/CERTFR-2014-ACT-043/

3 - Rappel des avis émis

Dans la période du 09 au 15 mars 2015, le CERT-FR a émis les publications suivantes :

- CERTFR-2015-AVI-090 : Multiples vulnérabilités dans les produits SCADA Siemens
- CERTFR-2015-AVI-091 : Vulnérabilité dans VLC Media Player
- CERTFR-2015-AVI-092 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2015-AVI-093 : Multiples vulnérabilités dans le noyau Linux de Red Hat
- CERTFR-2015-AVI-094 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2015-AVI-095 : Vulnérabilité dans le moteur de script VBScript de Windows
- CERTFR-2015-AVI-096 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2015-AVI-097 : Multiples vulnérabilités dans le pilote de fontes Adobe de Windows
- CERTFR-2015-AVI-098 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2015-AVI-099 : Multiples vulnérabilités dans le noyau de Windows
- CERTFR-2015-AVI-100 : Vulnérabilité dans le traitement des images PNG de Windows
- CERTFR-2015-AVI-101 : Multiples vulnérabilités dans le noyau de Windows
- CERTFR-2015-AVI-102 : Multiples vulnérabilités dans Microsoft Exchange Server
- CERTFR-2015-AVI-103 : Vulnérabilité dans le service Netlogon de Windows
- CERTFR-2015-AVI-104 : Vulnérabilité dans le composant Task Scheduler de Windows

- CERTFR-2015-AVI-105 : Vulnérabilité dans le traitement des fichiers JPEG de Windows
- CERTFR-2015-AVI-106 : Vulnérabilité dans le protocole RDP de Windows
- CERTFR-2015-AVI-107 : Vulnérabilité dans le composant Schannel de Windows
- CERTFR-2015-AVI-108 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-109 : Multiples vulnérabilités dans Xen
- CERTFR-2015-AVI-110 : Multiples vulnérabilités dans Citrix XenServer
- CERTFR-2015-AVI-111 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2015-AVI-112 : Vulnérabilité dans le noyau Linux d'Ubuntu
- CERTFR-2015-AVI-113 : Vulnérabilité dans Xen
- CERTFR-2015-AVI-114 : Multiples vulnérabilités dans Adobe Flash Flayer

Gestion détaillée du document

16 mars 2015 version initiale.