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 17 mai 2016
N° CERTFR-2016-ACT-020

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-020

1 - Mise à jour mensuelle de Microsoft

Le 10 mai, lors de sa mise à jour mensuelle, Microsoft a publié seize bulletins de sécurité, dont huit considérés critiques et huit importants :

- MS16-051 (critique) concernant Internet Explorer ;
- MS16-052 (critique) concernant le navigateur Edge ;
- MS16-053 (critique) concernant JScript et VBScript ;
- MS16-054 (critique) concernant Microsoft Office ;
- MS16-055 (critique) concernant le composant Microsoft Graphics ;
- MS16-056 (critique) concernant le Journal Windows ;
- MS16-057 (critique) concernant Windows Shell ;
- MS16-064 (critique) concernant Adobe Flash Player ;
- MS16-058 (important) concernant Windows IIS ;
- MS16-059 (important) concernant Windows Media Center ;
- MS16-060 (important) concernant le noyau Windows ;
- MS16-061 (important) concernant Microsoft RPC ;
- MS16-062 (important) concernant les pilotes en mode noyau Windows ;
- MS16-065 (important) concernant le cadriciel .NET ;
- MS16-066 (important) concernant le mode sécurisé virtuel ;
- MS16-067 (important) concernant le pilote du Gestionnaire de volume.

Navigateurs

Cette mise à jour corrige cinq vulnérabilités considérées critiques dans Internet Explorer, dont trois permettent une exécution de code à distance.
A noter que deux d'entre elles concernent les moteurs de script JScript et VBScript (CVE-2016-0187 et CVE-2016-0189). De plus Microsoft indique que la vulnérabilité CVE-2016-0189 est activement exploitée.
La vulnérabilité CVE-2016-0188 permet de contourner une des fonctionnalités de sécurité d'Internet Explorer 11 sur Windows 10. En abusant le composant Intégrité du Code Mode Utilisateur (User Mode Code Integrity, UMCI) de Device Guard, un attaquant pourrait réussir à faire exécuter du code non-signé.
Microsoft a également corrigé la vulnérabilité CVE-2016-0194, comblant ainsi une erreur d'autorisation d'accès à des fichiers qui aurait pu permettre à un attaquant d'obtenir des informations potentiellement sensibles sur le système.

Le navigateur Edge reçoit quatre correctifs de sécurité. Les vulnérabilités CVE-2016-0186, CVE-2016-0191 et CVE-2016-0193 touchent le moteur Chakra Javascript lorsqu'il traite les objets en mémoire. Une exploitation réussie peut conduire à une exécution de code arbitraire.

La vulnérabilité CVE-2016-0192 est elle aussi dûe à une mauvaise gestion des objets en mémoire et peut également conduire à une exécution de code arbitraire. A noter que celle-ci touche également Internet Explorer.

Le 10 mai 2016, Adobe a émis une alerte au sujet d'une faille de type 0 jour dans Flash Player, reprise par le CERT-FR (CERTFR-2016-ALE-003). Activement exploitée, la CVE-2016-4117 permettait aussi une exécution de code arbitraire à distance. Le correctif de sécurité est disponible depuis le 12 mai et comble également 24 autres vulnérabilités.
Le greffon Flash Player pour les deux navigateurs de Microsoft étant également impactés, il est bien entendu nécessaire de procéder à la mise à jour.

Bureautique

Quatre vulnérabilités de type corruption de mémoire ont été corrigées dans Microsoft Office. Celles-ci sont susceptibles de permettre une exécution de code à distance lors de l'ouverture d'un fichier spécialement conçu. Les vulnérabilités CVE-2016-0183 et CVE-2016-0198 sont considérées critiques, alors que les CVE-2016-0126 et CVE-2016-0140 ont un niveau important.

Windows

En plus des vulnérabilités affectant les moteurs de script JScript et VBScript mentionnées dans le paragraphe dédiée à Internet Explorer, des composants internes de Windows sont concernés par trois autres bulletins notés critiques et sept jugés importants.
Le premier traite du composant Microsoft Graphics, dont cinq vulnérabilités ont été corrigées. Trois d'entre elles sont des exécutions de code arbitraire à distance. La CVE-2016-0184 est de type utilisation après libération et est actuellement activement exploitée. Les vulnérabilités CVE-2016-0170 et CVE-2016-0195 sont de type corruption de mémoire. Les deux dernières vulnérabilités touchant le composant Graphics peuvent permettre à un attaquant d'obtenir des informations sensibles sur le système (CVE-2016-0168 et CVE-2016-0169).

La vulnérabilité CVE-2016-0182 peut être exploitée par un fichier du journal Windows (.jnt) spécialement conçu, ce qui peut potentiellement permettre à un attaquant d'exécuter du code arbitraire dans le contexte de l'utilisateur actuel.

Le Windows Shell est impacté par la vulnérabilité critique CVE-2016-0179, dont l'exploitation peut déboucher sur une exécution de code arbitraire à distance. Par exemple, en incitant un utilisateur à visiter un site internet piégé, un attaquant pourrait déclencher la vulnérabilité pour prendre contrôle du système.

La vulnérabilité CVE-2016-0152 provient d'un chargement non sécurisé de certaines bibliothèques dans Windows IIS. Cela peut entraîner une exécution de code à distance. Microsoft juge la gravité de cette vulnérabilité importante.

C'est également le cas de la vulnérabilité CVE-2016-0185 qui, en cas d'ouverture d'un fichier de liaison Media Center (.mcl) malveillant, pourrait permettre à un attaquant d'exécuter son propre code sur la machine cible.

Un traitement incorrect de certains liens symboliques dans le noyau de Windows peut permettre une élévation de privilège par la modification de clés de Registre privilégiées. Cette vulnérabilité importante est désignée par la CVE-2016-0180.

Lorsque Windows traite des requêtes Remote Procedure Call (RPC), le moteur de représentation des données du réseau RPC peut libérer de la mémoire de manière incorrecte. Un attaquant peut donc envoyer des requêtes RPC mal formées afin d'exploiter cette vulnérabilité (CVE-2016-0178) pour élever ses privilèges et tenter de prendre le contrôle du système.

Sept vulnérabilités ont été corrigées dans les pilotes en mode noyau Windows. Quatre d'entre elles peuvent déboucher sur des élévations de privilèges dûes à une mauvaise gestion des objets en mémoire de la part de Win32k (CVE-2016-0171, CVE-2016-0173, CVE-2016-0174, CVE-2016-0175).
Les vulnérabilités CVE-2016-0176 et CVE-2016-0197 peuvent également permettre une élévation de privilège. En effet, le sous-système graphique dans DirectX (dxgkrnl.sys) présente également des problèmes de gestion des objets en mémoire.
La vulnérabilité CVE-2016-0175 concerne une possible fuite d'information qui pourrait permettre à un attaquant de contourner la disposition stochastique de l'espace d'adressage mémoire noyau (KASLR).

La vulnérabilité CVE-2016-0181 impacte le mode sécurisé virtuel de Windows. Un attaquant pourrait tenter d'obtenir des droits en lecture, écriture et exécution sur des pages mémoire en mode noyau, et ce même si la fonctionnalité d'intégrité du code de l'hyperviseur (HVCI) est activée. Le correctif rétablit la protection de l'intégrité du code.

La vulnérabilité CVE-2016-0190 provient du fait qu'une clé USB, montée par l'intermédiaire du protocole RDP via Microsoft RemoteFX, ne lie pas correctement ce volume à la session de l'utilisateur. Un attaquant pourrait ainsi en profiter pour accéder aux données présentes sur ce support de stockage de masse.

Le cadriciel .NET est affecté par la vulnérabilité CVE-2016-0149. Un attaquant pourrait effectuer une interception active (MiTM) pour tenter de déchiffrer des communications sécurisées. Cela est dû à une faiblesse d'implémentation du protocole SSL/TLS du composant de chiffrement du cadriciel .NET. Microsoft a traité le problème en changeant la manière dont ce composant envoie et reçoit des paquets.

Recommandations

Le CERT-FR recommande l'application de ces correctifs de sécurité dès que possible.

Documentation

- Avis CERTFR-2016-AVI-162
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-162
- Avis CERTFR-2016-AVI-163
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-163
- Avis CERTFR-2016-AVI-164
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-164
- Avis CERTFR-2016-AVI-165
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-165
- Avis CERTFR-2016-AVI-169
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-169

2 - Rappel des avis émis

Dans la période du 09 au 15 mai 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-155 : Multiples vulnérabilités dans WordPress (09 mai 2016)
- CERTFR-2016-AVI-156 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu (09 mai 2016)
- CERTFR-2016-AVI-157 : Multiples vulnérabilités dans Squid (09 mai 2016)
- CERTFR-2016-AVI-158 : Multiples vulnérabilités dans Xen (10 mai 2016)
- CERTFR-2016-AVI-159 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu (10 mai 2016)
- CERTFR-2016-AVI-160 : Multiples vulnérabilités dans Adobe Coldfusion (11 mai 2016)
- CERTFR-2016-AVI-161 : Multiples vulnérabilités dans Adobe Acrobat et Reader (11 mai 2016)
- CERTFR-2016-AVI-162 : Multiples vulnérabilités dans Microsoft Edge (11 mai 2016)
- CERTFR-2016-AVI-163 : Multiples vulnérabilités dans Microsoft Office (11 mai 2016)
- CERTFR-2016-AVI-164 : Multiples vulnérabilités dans Microsoft Windows (11 mai 2016)
- CERTFR-2016-AVI-165 : Vulnérabilité dans Microsoft .NET Framework (11 mai 2016)
- CERTFR-2016-AVI-166 : Multiples vulnérabilités dans Google Chrome (12 mai 2016)
- CERTFR-2016-AVI-167 : Multiples vulnérabilités dans ArubaOS (12 mai 2016)
- CERTFR-2016-AVI-168 : Multiples vulnérabilités dans 7-Zip (12 mai 2016)
- CERTFR-2016-AVI-169 : Multiples vulnérabilités dans Microsoft Internet Explorer (12 mai 2016)
- CERTFR-2016-AVI-170 : Multiples vulnérabilités dans Adobe Flash Player (12 mai 2016)

Gestion détaillée du document

17 mai 2016 version initiale.