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 octobre 2016
N° CERTFR-2016-ACT-042

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-042

1 - Mise à jour mensuelle de Microsoft

Le 11 octobre, lors de sa mise à jour mensuelle, Microsoft a publié neuf bulletins de sécurité, dont cinq sont considérés comme critiques, trois comme importants et un comme modéré :

- MS16-118 (critique) concernant Internet Explorer ;
- MS16-119 (critique) concernant le navigateur Edge ;
- MS16-120 (critique) concernant le composant graphique (GDI) de Microsoft ;
- MS16-121 (critique) concernant Microsoft Office ;
- MS16-122 (critique) concernant le contrôle vidéo de Windows ;
- MS16-123 (important) concernant les pilotes en mode noyau Windows ;
- MS16-124 (important) concernant le registre de Windows ;
- MS16-125 (important) concernant le concentrateur de diagnostic ;
- MS16-126 (modéré) concernant l'API Microsoft Internet Messaging ;

Navigateurs

Cette mise à jour corrige douze vulnérabilités dans Internet Explorer. Six permettent une exécution de code à distance et sont considérées comme critiques. Ce so nt des vulnérabilités qui sont déclenchées par des corruptions de mémoire. Parmi les restantes, trois autres vulnérabilités débouchent sur des fuites d'information, et deux autres sur une élévation de privilèges. La dernière, la CVE-2016-3298, permet la divulgation d'informations par le biais de l'API Microsoft Internet Messaging dans Internet Explorer.

Treize vulnérabilités ont été corrigées dans Microsoft Edge. Sept permettent une exécution de code à distance, trois autres une fuite d'information, deux autres une élévation de privilèges et la dernière permet un contournement de la politique de sécurité.

Trois des vulnérabilités permettant une exécution de code à distance sont partagées avec Internet Explorer : il s'agit des vulnérabilités CVE-2016-3331, CVE2016-3382 et CVE-2016-3390. Parmi celles permettant une élévation de privilèges, deux d'entre elles sont partagées avec Internet Explorer : il s'agit des vulnérabilités CVE-2016-3387 et CVE-2016-3388 considérées comme importantes.

Bureautique

Office reçoit un seul correctif de sécurité qui concerne Microsoft Office dans ses versions 2007, 2010, 2013 et 2016 pour Windows, 2011 et 2016 pour Mac. La vulnérabilité CVE-2016-7193 corrigée permet une exécution de code à distance si l'utilisateur ouvre un fichier piégé ou se rend sur un site Internet malveillant. Cette vulnérabilité est notée comme critique.

Windows

Six vulnérabilités affectant le composant graphique de Windows (GDI) ont été corrigées. Une d'entre elles (CVE-2016-3393) est jugée critique et permet une exécution de code à distance si l'utilisateur ouvre un fichier piégé ou se rend sur un site Internet malveillant. Deux d'entre elles (CVE-2016-3209 et CVE-2016-7182) sont importantes et peuvent être exploitées par une police de caractères spécialement forgée afin d'exécuter du code à distance. Les trois restantes (CVE-2016-3209, CVE-2016-3262 et CVE-2016-3263) permettent une divulgation d'informations du système ciblé, et éventuellement une exécution de code arbitraire en combinaison avec une autre vulnérabilité permettant de contourner la distribution stochastique de l'espace d'adressage (ASLR). À noter que ces vulnérabilités impactent toutes les versions de Windows, mais également Office, Skype, Lync, le cadriciel Microsoft .NET et Silverlight.

La vulnérabilité CVE-2016-0142 impacte le contrôle vidéo de Windows de manière critique et permet une exécution de code à distance si l'utilisateur ouvre un fichier piégé à partir d'une page web ou d'un message électronique.

Six vulnérabilités dans Win32K peuvent déclencher une élévation de privilèges : CVE-2016-3266, CVE-2016-3270, CVE-2016-3341, CVE-2016-3376, CVE-2016-7185 et CVE-2016-7211. Un attaquant authentifié localement devrait exécuter une application spécialement conçue pour exploiter ces vulnérabilités.

Quatre vulnérabilités dans le noyau Windows permettent une élévation de privilèges : CVE-2016-0070, CVE-2016-0073, CVE-2016-0075 et CVE-2016-0079. Une mauvaise vérification des autorisations de lecture au registre de Windows est à l'origine de ces vulnérabilités.

Enfin, la vulnérabilité CVE-2016-7188 permet d'élever ses privilèges dans le service "Collecteur standard du concentrateur de diagnostic Windows" de Windows 10 lorsque celui-ci nettoie partiellement ses entrées, pouvant mener à un chargement de bibliothèque non sécurisé.

Recommandations

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

Documentation

- https://technet.microsoft.com/fr-fr/library/security/MS16-118
- https://technet.microsoft.com/fr-fr/library/security/MS16-119
- https://technet.microsoft.com/fr-fr/library/security/MS16-120
- https://technet.microsoft.com/fr-fr/library/security/MS16-121
- https://technet.microsoft.com/fr-fr/library/security/MS16-122
- https://technet.microsoft.com/fr-fr/library/security/MS16-123
- https://technet.microsoft.com/fr-fr/library/security/MS16-124
- https://technet.microsoft.com/fr-fr/library/security/MS16-125
- https://technet.microsoft.com/fr-fr/library/security/MS16-126

2 - Rappel des avis émis

Dans la période du 10 au 16 octobre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-334 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-335 : Vulnérabilité dans Quagga
- CERTFR-2016-AVI-336 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2016-AVI-337 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-338 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-339 : Vulnérabilité dans Microsoft Office
- CERTFR-2016-AVI-340 : Multiples vulnérabilités dans Microsoft Windows

- CERTFR-2016-AVI-341 : Multiples vulnérabilités dans le smartphone P9 Huawei
- CERTFR-2016-AVI-342 : Multiples vulnérabilités dans Ghostscript
- CERTFR-2016-AVI-343 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-344 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2016-AVI-345 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-346 : Multiples vulnérabilités dans Apache OpenOffice
- CERTFR-2016-AVI-347 : Multiples vulnérabilités dans les produits Siemens

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

- CERTFR-2016-ALE-006 : Campagne de messages électroniques non sollicités de type Zepto/Odin (ajout marqueurs supplémentaires ;)

Gestion détaillée du document

17 octobre 2016 version initiale.