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 novembre 2016
N° CERTFR-2016-ACT-046

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-046

1 - Mise à jour mensuelle de Microsoft

Le 8 novembre, lors de sa mise à jour mensuelle, Microsoft a publié quatorze bulletins de sécurité, dont six sont considérés comme critiques et huit comme importants :

- MS16-129 (critique) concernant le navigateur Edge ;
- MS16-130 (critique) concernant Microsoft Windows ;
- MS16-131 (critique) concernant le contrôle vidéo Microsoft ;
- MS16-132 (critique) concernant le composant Microsoft Graphics ;
- MS16-141 (critique) concernant Adobe Flash Player ;
- MS16-142 (critique) concernant Internet Explorer ;
- MS16-133 (important) concernant Microsoft Office ;
- MS16-134 (important) concernant le pilote Common Log File System ;
- MS16-135 (important) concernant les pilotes en mode noyau Windows ;
- MS16-136 (important) concernant SQL Server ;
- MS16-137 (important) concernant les méthodes d'authentification Windows ;
- MS16-138 (important) concernant le pilote de disque dur virtuel Microsoft ;
- MS16-139 (important) concernant le noyau Windows ;
- MS16-140 (important) concernant le gestionnaire de démarrage ;

Navigateurs

Cette mise à jour corrige sept vulnérabilités dans Internet Explorer. Quatre permettent une exécution de code à distance et sont considérées comme critiques. Ce sont des vulnérabilités qui sont déclenchées par des corruptions de mémoire.
Les trois autres vulnérabilités débouchent sur des fuites d'informations. Leur sévérité est jugée d'importante à faible selon les contextes. Dix-sept vulnérabilités ont été corrigées dans Microsoft Edge. Douze permettent une exécution de code à distance et sont considérées comme critiques, à une exception près qui est jugée importante. Parmi ces vulnérabilités, quatre proviennent de possibles altérations de mémoire dans le navigateur et les huit autres sont situées au niveau du moteur de scripts.
Quatre autres sont de type fuite d'informations. La dernière vulnérabilité corrigée dans Edge permet d'usurper l'identité d'un site internet en permettant d'afficher une URL différente de celle réellement demandée. Celle-ci portant l'identifiant CVE-2016-7209 a été révélée publiquement.
Sept vulnérabilités sont communes à Internet Explorer et à Edge : la CVE-2016-7195, CVE-2016-7196, CVE-2016-7198 et CVE-2016-7241 sont de type exécution de code à distance, les trois autres de type fuite d'informations. Parmi celles-ci, la vulnérabilité CVE-2016-7199 a été révélée publiquement. Adobe a corrigé neuf vulnérabilités pouvant conduire à des exécutions de code à distance pour son Flash Player dans Internet Explorer et Edge. Sept d'entre elles sont considérées comme critiques.

Bureautique

Office reçoit douze correctifs de sécurité. Dix d'entre elles proviennent de possibles altérations de mémoire pouvant conduire à une exécution de code à distance. La CVE-2016-7233 est une vulnérabilité de divulgation d'informations qui permet à un attaquant de lire du contenu mémoire supposé non accessible en raison d'une variable non initialisée. La dernière vulnérabilité impactant Office est de type déni de service.

Windows

Parmi les vulnérabilités critiques touchant le système Windows, quatre permettent une exécution de code à distance. La vulnérabilité CVE-2016-7212 peut être déclenchée par un fichier image mal formé. La vulnérabilité CVE-2016-7248 se situe dans le contrôle vidéo de Windows. La vulnérabilité CVE-2016-7205 impacte de Gestionnaire d'animations de Windows et sa manière de gérer les objets en mémoire. Enfin la vulnérabilité CVE-2016-7256 peut-être exploitée par une police incorporée spécialement conçue.

La vulnérabilité CVE-2016-7217 permet une exécution de code à distance jugée importante. Il s'agit d'une potentielle altération de mémoire dans Windows Media Foundation.

Vingt-et-une vulnérabilités permettant une élévation de privilèges ont été corrigées dans différents composants de Windows. La plus notable est la CVE-2016-7255 que Google a annoncée publiquement la semaine dernière et qui faisait l'objet d'une exploitation active dans le cadre d'attaques ciblées.

Six autres vulnérabilités ont également été corrigées dans Windows, dont quatre de type divulgation d'informations, une de contournement de la politique de sécurité (CVE-2016-7247) et enfin une pouvant déboucher sur un déni de service(CVE-2016-7237).

Pour finir, six vulnérabilités impactent le SQL Server: quatre d'élévations de privilèges, une de divulgation d'informations et une de script inter-sites (XSS).

Recommandations

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

Documentation

- https://technet.microsoft.com/fr-fr/library/security/MS16-129
- https://technet.microsoft.com/fr-fr/library/security/MS16-130
- https://technet.microsoft.com/fr-fr/library/security/MS16-131
- https://technet.microsoft.com/fr-fr/library/security/MS16-132
- https://technet.microsoft.com/fr-fr/library/security/MS16-133
- https://technet.microsoft.com/fr-fr/library/security/MS16-134
- https://technet.microsoft.com/fr-fr/library/security/MS16-135
- https://technet.microsoft.com/fr-fr/library/security/MS16-136
- https://technet.microsoft.com/fr-fr/library/security/MS16-137
- https://technet.microsoft.com/fr-fr/library/security/MS16-138
- https://technet.microsoft.com/fr-fr/library/security/MS16-139
- https://technet.microsoft.com/fr-fr/library/security/MS16-140
- https://technet.microsoft.com/fr-fr/library/security/MS16-141
- https://technet.microsoft.com/fr-fr/library/security/MS16-142

2 - Rappel des avis émis

Dans la période du 07 au 13 novembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-369 : Vulnérabilité dans SCADA les produits Siemens
- CERTFR-2016-AVI-370 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-371 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2016-AVI-372 : Multiples vulnérabilités dans Microsoft Internet Explorer

– CERTFR-2016-AVI-373 : Multiples vulnérabilités dans Microsoft Edge
– CERTFR-2016-AVI-374 : Multiples vulnérabilités dans Microsoft Windows
– CERTFR-2016-AVI-375 : Multiples vulnérabilités dans Microsoft Office

Durant la même période, les publications suivantes ont été mises à jour :
– CERTFR-2016-ALE-008 : Vulnérabilité dans Microsoft Windows (clôture de l'alerte.)

Gestion détaillée du document

14 novembre 2016 version initiale.
21 novembre 2016 correction copié/collé.