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 19 décembre 2016
N° CERTFR-2016-ACT-051

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-051

1 - Mise à jour mensuelle de Microsoft

Le 13 décembre, lors de sa mise à jour mensuelle, Microsoft a publié douze bulletins de sécurité, dont six sont considérés comme critiques et six comme importantes :

- MS16-144 (critique) concernant Internet Exlorer ;
- MS16-145 (critique) concernant le navigateur Edge ;
- MS16-146 (critique) concernant le composant Microsoft Graphics ;
- MS16-147 (critique) concernant Microsoft Uniscribe ;
- MS16-148 (critique) concernant Microsoft Office ;
- MS16-154 (critique) concernant Adobe Flash Player ;
- MS16-149 (important) concernant Microsoft Windows ;
- MS16-150 (important) concernant le mode de noyau sécurisé ;
- MS16-151 (important) concernant les pilotes en mode noyau Windows ;
- MS16-152 (important) concernant le noyau Windows ;
- MS16-153 (important) concernant le pilote Common Log File System ;
- MS16-155 (important) concernant le cadriciel .NET.

Navigateurs

Cette mise à jour corrige huit vulnérabilités dans Internet Explorer. Quatre permettent une exécution de code à distance et sont considérées comme critiques, à une exception près qui est jugée importante. Ces vulnérabilités sont déclenchées par des corruptions de mémoire. La vulnérabilité CVE-2016-7202 exploite notamment une altération de la mémoire dans le moteur de script et a été révélée publiquement avant la publication du correctif.

Trois autres vulnérabilités débouchent sur des fuites d'informations. Leur sévérité est jugée importante.

Enfin, une dernière vulnérabilité importante permet un contournement de la politique d'origine commune (*Same Origin Policy*), qui évite qu'un script malveillant téléchargé depuis un certain domaine accède aux données liées à d'autres domaines, tels que les cookies de session.

Onze vulnérabilités ont été corrigées dans Microsoft Edge. Sept permettent une exécution de code à distance et parmi celles-ci, quatre sont considérées comme critiques, deux sont jugées importantes et une modérée. Parmi ces vulnérabilités, deux proviennent de possibles altérations de mémoire dans le navigateur et les cinq autres sont situées au niveau du moteur de script. Ces vulnérabilités pourraient être exploitées par un attaquant *via* une page Web malveillante.

Trois vulnérabilités corrigées conduisent à une divulgation d'informations. Jugées comme importantes, ces vulnérabilités tirent parti d'une validation incorrecte du contenu. Deux d'entre elles, les CVE-2016-7206 et CVE-2016-7282 ont été révélées publiquement.

La dernière vulnérabilité corrigée dans Edge permet de contourner la politique d'origine commune (*Same Origin Policy*).

Quatre vulnérabilités sont communes à Internet Explorer et à Edge. La CVE-2016-7287, considérée comme critique, permet une altération de la mémoire dans le moteur de script et entraîne une exécution de code à distance. Les trois autres, les CVE-2016-7279, CVE-2016-7281 et CVE-2016-7282, sont considérées comme importantes et provoquent respectivement une altération de la mémoire du navigateur, un contournement de la fonctionnalité de sécurité et une divulgation d'informations.

Adobe a corrigé seize vulnérabilités pouvant conduire à des exécutions de code à distance pour le logiciel Flash Player dans Internet Explorer et Edge. Considérées comme critiques, ces vulnérabilités peuvent conduire à une exécution de code à distance.

Bureautique

Office reçoit seize correctifs de sécurité. Quatre d'entre elles proviennent de possibles altérations de mémoire pouvant conduire à une exécution de code à distance. De plus, la vulnérabilité CVE-2016-7275 autorise là aussi une possible exécution de code.

Trois vulnérabilités permettent un contournement de la politique de sécurité de Microsoft Office. En particulier, la CVE-2016-7267 touche une fonctionnalité en charge de l'analyse du format de fichier.

Sept vulnérabilités sont liées à des divulgations d'informations et peuvent amener un attaquant à accéder à des zones mémoire hors limites. Parmi celles-ci, la CVE-2016-7257 pourrait amener à un contournement de la distribution aléatoire de l'espace d'adressage (*ASLR*).

Enfin, une dernière vulnérabilité affectant Microsoft Office peut conduire à une élévation de privilèges.

Windows

Dix vulnérabilités impactant Windows ont été corrigées.

Deux d'entre elles sont considérées comme critiques et peuvent provoquer une exécution de code à distance. Ces deux vulnérabilités affectent le composant *Graphics* de Windows. L'une d'elles, la vulnérabilité CVE-2016-7273, est connue pour être exploitée. Cette vulnérabilité pourrait être exploitée en passant par une page Web malveillante créée par l'attaquant.

Les huit autres vulnérabilités recensées sont jugées importantes. Parmi celles-ci, quatre peuvent conduire à une élévation de privilèges. Les CVE-2016-7259 et CVE-2016-7260 ciblent notamment une vulnérabilité dans *Win32k*.

Enfin, les quatre autres vulnérabilités impliquent un risque de divulgation d'informations. La CVE-2016-7258 pourrait en particulier conduire à communiquer de façon abusive de l'information d'un processus à un autre.

Recommandations

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

Documentation

- https://technet.microsoft.com/fr-fr/library/security/MS16-144
- https://technet.microsoft.com/fr-fr/library/security/MS16-145
- https://technet.microsoft.com/fr-fr/library/security/MS16-146
- https://technet.microsoft.com/fr-fr/library/security/MS16-147
- https://technet.microsoft.com/fr-fr/library/security/MS16-148
- https://technet.microsoft.com/fr-fr/library/security/MS16-149
- https://technet.microsoft.com/fr-fr/library/security/MS16-150

- https://technet.microsoft.com/fr-fr/library/security/MS16-151
- https://technet.microsoft.com/fr-fr/library/security/MS16-152
- https://technet.microsoft.com/fr-fr/library/security/MS16-153
- https://technet.microsoft.com/fr-fr/library/security/MS16-154
- https://technet.microsoft.com/fr-fr/library/security/MS16-155

2 - Rappel des avis émis

Dans la période du 12 au 18 décembre 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-ALE-010 : Vulnérabilité dans les routeurs Netgear
- CERTFR-2016-AVI-406 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2016-AVI-407 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2016-AVI-408 : Multiples vulnérabilités dans McAfee VirusScan Enterprise
- CERTFR-2016-AVI-409 : Vulnérabilité dans Adobe ColdFusion Builder
- CERTFR-2016-AVI-410 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2016-AVI-411 : Multiples vulnérabilités dans les produits Apple
- CERTFR-2016-AVI-412 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-413 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-414 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-415 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2016-AVI-416 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-417 : Vulnérabilité dans Microsoft .NET Framework
- CERTFR-2016-AVI-418 : Vulnérabilité dans Xen
- CERTFR-2016-AVI-419 : Multiples vulnérabilités dans Joomla!
- CERTFR-2016-AVI-420 : Multiples vulnérabilités dans le noyau Linux de SUSE

Gestion détaillée du document

19 décembre 2016 version initiale.