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 août 2016
N° CERTFR-2016-ACT-033

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-033

1 - Mise à jour mensuelle de Microsoft

Le 09 août, lors de sa mise à jour mensuelle, Microsoft a publié neuf bulletins de sécurité, dont cinq sont considérés comme critiques et quatre comme importants :

- MS16-095 (critique) concernant Internet Explorer ;
- MS16-096 (critique) concernant le navigateur Edge ;
- MS16-097 (critique) concernant le composant graphique (GDI) de Microsoft ;
- MS16-099 (critique) concernant Microsoft Office ;
- MS16-102 (critique) concernant la bibliothèque PDF de Windows ;
- MS16-098 (important) concernant les pilotes en mode noyau Windows ;
- MS16-100 (important) concernant le démarrage sécurisé ;
- MS16-101 (important) concernant les méthodes d'authentification de Windows ;
- MS16-103 (important) concernant ActiveSyncProvider ;

Navigateurs

Cette mise à jour corrige neuf vulnérabilités dans Internet Explorer. Cinq permettent une exécution de code à distance et quatre d'entre elles sont considérées comme critiques. Ce sont des vulnérabilités qui sont déclenchées par des corruptions de mémoire.

Les quatre autres vulnérabilités débouchent sur des fuites d'information.

Huit vulnérabilités ont été corrigées dans Microsoft Edge. Cinq permettent une exécution de code à distance et les trois autres une fuite d'information.

Trois des vulnérabilités permettant une exécution de code à distance sont partagées avec Internet Explorer : il s'agit des vulnérabilités CVE-2016-3289, CVE-2016-3293 et CVE-2016-3322. À noter que dans le contexte d'Edge, la vulnérabilité CVE-2016-3293 n'est pas considérée comme critique, mais importante.

Bureautique

Office reçoit cinq correctifs de sécurité. Quatre concernent des exécutions de code à distance possibles si l'utilisateur ouvre un fichier piégé ou se rend sur un site Internet malveillant. La vulnérabilité CVE-2016-3316 est notée critique, les autres sont considérées importantes.

La vulnérabilité CVE-2016-3315 impacte le logiciel OneNote et permet à un attaquant d'obtenir des informations sur le contenu de la mémoire.

Windows

Trois vulnérabilités affectant le composant graphique de Windows (GDI) ont été corrigées. Celles-ci (CVE-2016-3301, CVE-2016-3303 et CVE-2016-3304) peuvent être exploitées par une police de caractère spécialement forgée et déboucher sur une exécution de code à distance jugée critique. À noter que ces vulnérabilités impactent toutes les versions de Windows, mais également Office, Skype et Lync.

La vulnérabilité CVE-2016-3319 impacte la bibliothèque PDF de Windows de manière critique et permet une exécution de code à distance. Celle-ci peut également être exploitée dans le contexte d'Edge.

Quatre vulnérabilités dans Win32K peuvent déclencher une élévation de privilège : CVE-2016-3308,CVE-2016-3309, CVE-2016-3310 et CVE-2016-3311.

La vulnérabilité CVE-2016-3320 permet un contournement du Windows Secure Boot, ce qui permet de désactiver les contrôles d'intégrité du code de Windows au démarrage, et ce même si la machine est protégée et chiffrée par BitLocker.

La vulnérabilité CVE-2016-3237 permet d'élever ses privilèges en exploitant une faille dans Kerberos alors que la vulnérabilité CVE-2016-3300 abuse NetLogon pour obtenir le même résultat.

Enfin, l'exploitation de la vulnérabilité CVE-2016-3312 permet à un attaquant d'obtenir l'identifiant ainsi que le mot de passe d'un utilisateur dans le cas où le logiciel Universal Outlook n'établirait pas une connexion sécurisée.

Recommandations

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

2 - Rappel des avis émis

Dans la période du 07 au 15 août 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-266 : Multiples vulnérabilités dans le noyau Linux SUSE
- CERTFR-2016-AVI-267 : Multiples vulnérabilités dans le noyau Linux SUSE
- CERTFR-2016-AVI-268 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-269 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-270 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2016-AVI-271 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-272 : Multiples vulnérabilités dans le noyau Linux d'Oracle
- CERTFR-2016-AVI-273 : Multiples vulnérabilités dans la bibliothèque GNU C (glibc)
- CERTFR-2016-AVI-274 : Vulnérabilité dans Xen QEMU
- CERTFR-2016-AVI-275 : Multiples vulnérabilités dans les noyaux Linux de Red Hat
- CERTFR-2016-AVI-276 : Vulnérabilité dans les produits Huawei
- CERTFR-2016-AVI-277 : Vulnérabilité dans Huawei Unified Security Gateway
- CERTFR-2016-AVI-278 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2016-AVI-279 : Multiples vulnérabilités dans OpenSSH
- CERTFR-2016-AVI-280 : Multiples vulnérabilités dans les produits F5 BIG-IP
- CERTFR-2016-AVI-281 : Multiples vulnérabilités dans PostgreSQL

Gestion détaillée du document

16 août 2016 version initiale.