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 août 2017
N° CERTFR-2017-ACT-032

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-032

1 - Mise à jour mensuelle de Microsoft

Le 08 août 2017, Microsoft a publié ses mises à jour mensuelles de sécurité. Quarante-neuf vulnérabilités ont été corrigées, parmi lesquelles vingt-six sont considérées critiques, vingt-et-une sont considérées importantes et deux sont considérées modérées.

Les produits suivants sont affectés :

- Internet Explorer ;
- Microsoft Edge ;
- Microsoft Windows ;
- Microsoft SharePoint ;
- Adobe Flash Player ;
- Microsoft SQL Server.

Navigateurs

Sept vulnérabilités sont corrigées dans Internet Explorer lors de cette mise à jour. Six permettent une exécution de code à distance, dont cinq sont jugées critiques. Ces vulnérabilités proviennent du moteur de script ou de la gestion des objets en mémoire par le navigateur.

La vulnérabilité CVE-2017-8651 peut permettre à un logiciel malveillant de contourner les politiques d'intégrité de code en mode utilisateur (*User Mode Code Integrity - UMCI*) de *Device Guard*.

Vingt-neuf correctifs sont apportés au navigateur Microsoft Edge. Parmi les vulnérabilités rapportées, vingt-et-une concernent des exécutions de code à distance. Ces vulnérabilités sont toutes définies comme critiques par Microsoft. Cinq de ces vulnérabilités sont communes à Internet Explorer et à Edge : CVE-2017-8635, CVE-2017-8636, CVE-2017-8641, CVE-2017-8653 et CVE-2017-8669.

Quatre vulnérabilités de divulgation d'information ont également été corrigées, tout comme deux vulnérabilités d'élévation de privilèges et deux vulnérabilités de contournement de la fonctionnalité de sécurité.

En plus de ces correctifs pour les navigateurs, la publication du mois d'août de Microsoft intègre un correctif d'Adobe pour le module Flash Player intégré dans Internet Explorer et Edge. Les vulnérabilités corrigées sont jugées comme critiques et peuvent conduire à une exécution de code arbitraire à distance.

Windows

Les correctifs Microsoft pour le mois d'août 2017 corrigent seize failles de sécurité pour Windows.

Seize vulnérabilités ont été corrigées dans Microsoft Windows. Six d'entre elles permettent des exécutions de code arbitraire à distance et quatre sont notées critiques. Parmi elles, La vulnérabilité CVE-2017-8591 impacte l'éditeur de méthode d'entrée (*IME*).
La vulnérabilité CVE-2017-0293 est présente dans les bibliothèques *PDF*. Cette vulnérabilité peut être déclenchée par l'ouverture d'un document `.pdf` piégé ou lors de l'ouverture d'une page web embarquant du contenu *PDF* malveillant ; ce dernier cas ne fonctionne que si Edge est défini comme le navigateur par défaut.
La vulnérabilité CVE-2017-0250 est due à un débordement de tampon dans le moteur de base de données Microsoft JET.
La vulnérabilité CVE-2017-8620 permet également une exécution de code arbitraire à distance par le biais d'une requête Windows Search. A noter que cette vulnérabilité peut être exploitée par le biais d'une requête SMB, et ce même si ce service n'est pas vulnérable dans ce cas.

Quatre vulnérabilités d'élévation de privilège ont été corrigées, dont la vulnérabilité CVE-2017-8622. Celle-ci est due à la gestion des tubes NT par le sous-système Windows pour Linux. La vulnérabilité CVE-2017-8633 a été révélée publiquement et permet également d'obtenir une élévation de privilèges.

A cela s'ajoutent deux vulnérabilités de divulgation d'information et quatre vulnérabilité permettant un déni de service. Parmi ces dernières, la vulnérabilité CVE-2017-8633 a également été dévoilée publiquement.

La vulnérabilité CVE-2017-8654 permet une usurpation d'identité sur Microsoft Sharepoint. Pour finir, un attaquant peut exploiter la vulnérabilité CVE-2017-8516 pour obtenir l'accès à des tables normalement protégées sur Microsoft SQL Server.

Recommandations

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

Documentation

- Bulletin de sécurité Microsoft b3d96835-f651-e711-80dd-000d3a32fc99 du 08 août 2017
  https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/b3d96835-f651-e711-80dd-000d3a32fc99

2 - Rappel des avis émis

Dans la période du 07 août au 13 août 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-248 : Multiples vulnérabilités dans SCADA Siemens Mobilett Mira Max
- CERTFR-2017-AVI-249 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-250 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu
- CERTFR-2017-AVI-251 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2017-AVI-252 : Vulnérabilité dans les produits Netsarang
- CERTFR-2017-AVI-253 : Multiples vulnérabilités dans Fortinet FortiOS et FortiWeb
- CERTFR-2017-AVI-254 : Multiples vulnérabilités dans Adobe Reader et Acrobat
- CERTFR-2017-AVI-255 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2017-AVI-256 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2017-AVI-257 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2017-AVI-258 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2017-AVI-259 : Vulnérabilité dans Microsoft SQL Server
- CERTFR-2017-AVI-260 : Vulnérabilité dans Microsoft SharePoint
- CERTFR-2017-AVI-261 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2017-AVI-262 : Multiples vulnérabilités dans le noyau Linux de RedHat
- CERTFR-2017-AVI-263 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-264 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

14 août 2017 version initiale.

17 août 2017 correction de statistiques.

Conditions d'utilisation de ce document :	http://cert.ssi.gouv.fr/cert-fr/apropos.html
Dernière version de ce document :	http://cert.ssi.gouv.fr/site/CERTFR-2017-ACT-032