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 juillet 2017
N° CERTFR-2017-ACT-028

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-028

1 - Mise à jour mensuelle de Microsoft

Le 11 juillet 2017, Microsoft a publié ses mises à jour mensuelles de sécurité. Cinquante-huit vulnérabilités ont été corrigées, parmi lesquelles dix-neuf sont considérées critiques et trente-six sont considérées importantes.

Les produits suivants sont affectés :

- Internet Explorer ;
- Microsoft Edge ;
- Microsoft Windows ;
- Microsoft Office et Microsoft Office Services et Web Apps ;
- .NET Framework ;
- Adobe Flash Player ;
- Microsoft Exchange Server ;

Navigateurs

Sept vulnérabilités sont corrigées dans Internet Explorer lors de cette mise à jour. Cinq sont considérées comme critiques et concernent toutes une possibilité d'exécution de code à distance.

Les deux autres vulnérabilités corrigées pour le navigateur sont jugées importantes. La première, la CVE-2017-8592, entraîne un contournement de la politique de sécurité avec notamment la possibilité de contourner les restrictions de redirection CORS (*Cross-Origin Resource Sharing*). La seconde vulnérabilité permet une usurpation d'identité et est identifiée sous la référence CVE-2017-8602. Cette dernière vulnérabilité avait été révélée publiquement avant la parution du correctif de ce mois de juillet.

Dix-huit correctifs sont apportés au navigateur Microsoft Edge. Parmi les vulnérabilités rapportées, quatorze concernent des exécutions de code à distance. Ces vulnérabilités sont toutes définies comme critiques par Microsoft.

Deux vulnérabilités induisent un contournement des fonctionnalités de sécurité. Référencées comme CVE-2017-8592 et CVE-2017-8599, ces vulnérabilités sont considérées comme importantes. On notera que la CVE-2017-8592 impacte aussi le navigateur Internet Explorer.

Enfin, deux failles corrigées sont relatives à un problème d'usurpation d'identité. La première vulnérabilité, la CVE-2017-8601, apparait comme importante. La seconde, la CVE-2017-8611, est elle de sévérité modérée. Bien que non exploitées d'après les informations de Microsoft, ces deux vulnérabilités ont été révélées publiquement avant la publication d'un correctif.

En plus de ces correctifs pour les navigateurs, la publication du mois de juillet de Microsoft intègre un correctif d'Adobe pour le module Flash Player intégré dans Internet Explorer et Edge. Les trois vulnérabilités corrigées sont jugées comme critiques et peuvent conduire à une exécution de code arbitraire à distance. Il s'agit de la CVE-2017-3099, la CVE-2017-3080 et la CVE-2017-3100.

Bureautique

Cinq vulnérabilités sont corrigées dans Microsoft Office.

Les quatre premières correspondent à un risque d'exécution de code à distance et sont notées comme importantes par Microsoft. Le dernier correctif fourni est relatif à une vulnérabilité d'élévation de privilèges identifiée en tant que CVE-2017-8569.

Windows

Les correctifs Microsoft pour le mois de juillet 2017 corrigent trente failles de sécurité pour Windows.

Parmi les vulnérabilités recevant un correctif, trois sont catégorisées critiques. Il s'agit pour les trois de vulnérabilités d'exécution de code identifiées comme CVE-2017-8463, CVE-2017-8584 et CVE-2017-8589. La vulnérabilité CVE-2017-8584 affecte par exemple la solution HoloLens et peut être déclenchée *via* du trafic Wi-Fi malveillant conçu à cet effet. On notera que cette vulnérabilité avait déjà fait l'objet d'une divulgation publique.
En plus de ces vulnérabilités critiques, deux exécutions de code jugées importantes se voient apporter un correctif ce mois.

Parmi les autres correctifs, quinze concernent un risque d'élévation de privilèges. Ces vulnérabilités importantes peuvent affecter divers composants ou services de Windows tels que Win32k, DirectX ou encore le noyau Windows. Sept vulnérabilités corrigées sont relatives à des divulgations d'informations et sont considérées comme importantes à l'exception d'une de sévérité modérée. Parmi ces vulnérabilités importantes, la CVE-2017-8564 provoque une divulgation d'informations pouvant mener au contournement de la mesure de sécurité de disposition stochastique de l'espace d'adressage mémoire noyau (KASLR, *Kernel Address Space Layout Randomization*).

Enfin, les trois dernières vulnérabilités corrigées pour cette catégorie correspondent à un contournement des fonctionnalités de sécurité pour deux d'entre elles, et un possible déni de service pour la dernière. Ces trois vulnérabilités sont considérées comme importantes.

Recommandations

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

Documentation

- Bulletin de sécurité Microsoft du 11 juillet 2017
  https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/f2b16606-4945-e71180dc-000d3a32fc99

2 - Rappel des avis émis

Dans la période du 10 au 16 juillet 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-205 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2017-AVI-206 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2017-AVI-207 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2017-AVI-208 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2017-AVI-209 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2017-AVI-210 : Multiples vulnérabilités dans les produits Microsoft
- CERTFR-2017-AVI-211 : Vulnérabilité dans Nginx
- CERTFR-2017-AVI-212 : Multiples vulnérabilités dans les produits Juniper
- CERTFR-2017-AVI-213 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2017-AVI-214 : Vulnérabilité dans Samba
- CERTFR-2017-AVI-215 : Multiples vulnérabilités dans SCADA les produits OSIsoft
- CERTFR-2017-AVI-216 : Multiples vulnérabilités dans F5 BIG-IP

Gestion détaillée du document

17 juillet 2017 version initiale.

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-028