

Affaire suivie par :  
CERT-FR

## BULLETIN D'ACTUALITÉ

### Objet : Bulletin d'actualité CERTFR-2017-ACT-025

#### 1 - Mise à jour mensuelle de Microsoft

Le 13 juin 2017, Microsoft a publié ses mises à jour mensuelles de sécurité. Quatre-vingt-seize vulnérabilités ont été corrigées, parmi lesquelles dix-huit sont considérées critiques et soixante-seize sont considérées importantes.

Les produits suivants sont affectés :

- Internet Explorer ;
- Microsoft Edge ;
- Microsoft Windows ;
- Microsoft Office, Microsoft Office Services et Microsoft Office Web Apps ;
- Silverlight ;
- Skype pour les entreprises et Lync ;
- Adobe Flash Player.

#### Navigateurs

Six vulnérabilités pour Internet Explorer sont corrigées dans cette mise à jour. Parmi celles-ci, quatre permettent une exécution de code à distance dont trois considérées comme critiques et une importante. Les vulnérabilités critiques, identifiées comme CVE-2017-8517, CVE-2017-8522 et CVE-2017-8524, sont la conséquence de failles dans les moteurs de rendu JavaScript lorsqu'ils traitent les objets en mémoire.

Les deux autres vulnérabilités affectant Internet Explorer donnent lieu à des divulgations d'informations et sont jugées importantes par Microsoft.

Edge a reçu des correctifs pour dix-sept vulnérabilités. Dix failles critiques et une importante peuvent mener à une exécution de code. Pour ces vulnérabilités d'exécution de code, neuf trouvent leur origine dans le moteur de script JavaScript. Enfin, les vulnérabilités CVE-2017-8517, CVE-2017-8522 et CVE-2017-8524 corrigées dans Edge sont aussi connues pour impacter Internet Explorer.

Dans les autres correctifs apportés dans Edge, trois concernent de la divulgation d'informations, avec un impact allant de faible à important, et trois autres adressent des problèmes de contournement de la fonctionnalité de sécurité définis comme importants. Plus particulièrement, les CVE-2017-8523 et CVE-2017-8530, déjà connues publiquement, corrigent un contournement possible de la fonctionnalité *same-origin policy*.

Adobe a corrigé neuf vulnérabilités pour le module Flash Player intégré dans Internet Explorer et Edge. Jugées comme critiques, elles peuvent conduire à une exécution de code arbitraire à distance.

#### Bureautique

Vingt-huit vulnérabilités sont corrigées pour Office.

Douze de ces vulnérabilités permettent une exécution de code. Elles sont jugées comme critiques pour trois d'entre elles et importantes pour les neuf autres. Parmi les vulnérabilités considérées comme critique, la CVE-2017-0283 et la CVE-2017-8528 portent sur la gestion des objets en mémoire dans le composant *Uniscribe*.

Treize vulnérabilités importantes menant à de la divulgation d'informations sont corrigées dans les différents composants de Microsoft Office pour le mois de juin. En particulier, la CVE-2017-8550 adresse une vulnérabilité impactant Skype pour l'entreprise et Microsoft Lync.

Enfin, trois vulnérabilités importantes pouvant mener respectivement à une usurpation d'identité, une élévation de privilèges ou un contournement de la fonctionnalité de sécurité sont corrigées par Microsoft.

## Windows

Les correctifs du mois de juin corrigent soixante-cinq vulnérabilités pour Windows.

Neuf vulnérabilités peuvent conduire à une exécution de code. Huit d'entre elles sont considérées comme critiques par Microsoft et une comme importante. Parmi ces vulnérabilités, les CVE-2017-8464 et CVE-2017-8543 sont décrites comme étant exploitées. La première permet d'exécuter du code au travers d'un fichier .LNK malveillant quand la seconde vulnérabilité touche le service Windows Search.

Huit correctifs importants sont distribués pour des vulnérabilités d'élévation de privilèges et six, eux aussi classifiés comme importants par Microsoft, pour des problèmes de contournement de la fonctionnalité de sécurité. Sur ces six dernières vulnérabilités, cinq contournent les fonctionnalités fournies par *Device Guard*.

Quarante vulnérabilités liées à de la divulgation d'informations sont corrigées par ces mises à jour. Ces vulnérabilités sont toutes notées comme étant importantes.

Les deux dernières vulnérabilités pour Windows sont jugées importantes. La CVE-2017-8515, permet de provoquer un déni de service, alors que le CVE-2017-0295 permet de porter atteinte à l'intégrité des données.

## Correctifs additionnels

Outre les correctifs de sécurité pour les systèmes bénéficiant d'un support en cours, Microsoft a publié plusieurs correctifs pour des plateformes n'étant plus maintenues. Cela comprend notamment des correctifs de sécurité pour Windows XP et Windows Server 2003.

Les quinze vulnérabilités visées par ces correctifs additionnels provoquent toutes des exécutions de code et sont jugées comme critiques. Parmi celles-ci, plusieurs correspondent à des failles dévoilées publiquement par le groupe d'attaquants Shadow Brokers, à l'exemple de la CVE-2017-7269 affectant le module WebDAV d'un serveur IIS.

## Recommandations

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

## Documentation

- Bulletin de sécurité Microsoft du 13 juin 2017  
<https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/40969d56-1b2a-e711-80db-000d3a32fc99>
- Bulletin de sécurité Microsoft pour les correctifs additionnels du 13 juin 2017  
<https://blogs.technet.microsoft.com/msrc/2017/06/13/june-2017-security-update-release/>
- Conseils de sécurité additionnels de Microsoft du 13 juin 2017  
<https://technet.microsoft.com/en-us/library/security/4025685.aspx>
- Avis CERT-FR CERTFR-2017-AVI-181  
<http://cert.ssi.gouv.fr/site/CERTFR-2017-AVI-181/index.html>
- Alerte CERT-FR CERTFR-2017-ALE-008  
<http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-008/index.html>

## 2 - Rappel des avis émis

Dans la période du 12 au 18 juin 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-AVI-173 : Vulnérabilité dans Google Chrome
- CERTFR-2017-AVI-174 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2017-AVI-175 : Multiples vulnérabilités dans Adobe Flash Player et Shockwave Player
- CERTFR-2017-AVI-176 : Multiples vulnérabilités dans les produits Microsoft
- CERTFR-2017-AVI-177 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2017-AVI-178 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2017-AVI-179 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2017-AVI-180 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2017-AVI-181 : Multiples vulnérabilités dans les systèmes d'exploitation Microsoft Windows obsolètes
- CERTFR-2017-AVI-182 : Multiples vulnérabilités dans Mozilla Thunderbird
- CERTFR-2017-AVI-183 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2017-AVI-184 : Multiples vulnérabilités dans ISC BIND

## Gestion détaillée du document

**19 juin 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-025>

---