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 15 mai 2017
N° CERTFR-2017-ACT-020

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2017-ACT-020

1 - Mise à jour mensuelle de Microsoft

Le 9 mai 2017, Microsoft a publié ses mises à jour mensuelles de sécurité. Cinquante-six vulnérabilités ont été corrigées, parmi lesquelles quinze sont considérées critiques et quarante et une sont considérées importantes.

Les produits suivants sont affectés :

- Internet Explorer ;
- Microsoft Edge ;
- Microsoft Windows ;
- Microsoft Office et Services Microsoft Office et Microsoft Office Web Apps ;
- Le cadriciel .Net ;
- Adobe Flash Player.

Navigateurs

Cette mise à jour corrige six vulnérabilités dans Internet Explorer. Deux d'entre elles, les vulnérabilités CVE-2017-0222 et CVE-2017-0228, permettent une exécution de code à distance et sont considérées comme critiques. Les vulnérabilités CVE-2017-0226 et CVE-2017-0238 sont également de type exécution de code arbitraire à distance, mais sont considérées comme importantes. La vulnérabilité CVE-2017-0064 permet un contournement de la politique de sécurité, car du contenu non chiffré(HTTP) peut être chargé à partir d'emplacements chiffrés (HTTPS). La vulnérabilité CVE-2017-0231 corrige un problème dans le filtre Smartscreen et permet à un attaquant d'usurper l'identité d'un site en présentant à l'utilisateur une adresse différente de celle réellement visitée.

Edge a reçu quinze correctifs. Douze d'entre eux corrigent des vulnérabilités d'exécution de code arbitraire à distance. Parmi celles-ci, neuf sont considérées critiques. Deux vulnérabilités sont de type élévation de privilège (CVE-2017-0233 et CVE-2017-0241). La vulnérabilité d'usurpation d'identité CVE-2017-0231 qui impacte Internet Explorer a également été corrigée dans Edge.

Adobe a corrigé sept 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

Sept vulnérabilités sont corrigées pour Microsoft Office et services associés : six d'entre elles peuvent conduire à une exécution de code arbitraire à distance. Elles sont considérées comme importantes. Cependant, Microsoft indique que les vulnérabilités CVE-2017-0261 et CVE-2017-0262 ont été utilisées par des groupes d'attaquants dans le cadre d'attaques ciblées. La vulnérabilité CVE-2017-0255 est de type injection de code indirecte à distance (XSS) et permet une élévation de privilèges.

Windows

Trente vulnérabilités ont été corrigées dans les divers composants de Windows. Cinq d'entre elles sont critiques et permettent une exécution de code arbitraire à distance. Notamment, la vulnérabilité CVE-2017-0290 a fait l'objet d'une alerte du CERT-FR (cf. section Documentation). Pour rappel elle impacte les composants de sécurité de toutes les versions de Windows. Si cette vulnérabilité ne semble pas avoir été exploitée pour l'instant, le CERT-FR recommande de vérifier que ce correctif a bien été appliqué.

Les autres vulnérabilités sont de type divulgation d'information, déni de service et élévation de privilèges. D'ailleurs, la vulnérabilité d'élévation de privilège CVE-2017-0263 a été utilisée dans le cadre d'attaques ciblées, combinée aux vulnérabilités d'exécution de code à distance CVE-2017-0261 et CVE-2017-0262.

Enfin, la vulnérabilité critique CVE-2017-0248 est corrigée dans le cadriciel .NET et rend possible un contournement de la fonctionnalité de sécurité.

Recommandations

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

Documentation

- Bulletin de sécurité Microsoft du 9 mai 2017
  https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/bc365363-f51e-e71180da-000d3a32fc99
- Alerte CERT-FR CERTFR-2017-ALE-009
  http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-009/

2 - Rappel des avis émis

Dans la période du 08 au 14 mai 2017, le CERT-FR a émis les publications suivantes :

- CERTFR-2017-ALE-009 : Vulnérabilité dans Microsoft Malware Protection Engine
- CERTFR-2017-ALE-010 : Propagation d'un rançongiciel exploitant les vulnérabilités MS17-010
- CERTFR-2017-ALE-011 : Campagne de messages électroniques non sollicités de type Jaff
- CERTFR-2017-AVI-140 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2017-AVI-141 : Multiples vulnérabilités dans le noyau Linux de Suse
- CERTFR-2017-AVI-142 : Vulnérabilité dans Mozilla Firefox
- CERTFR-2017-AVI-143 : Vulnérabilité dans les commutateurs Cisco
- CERTFR-2017-AVI-144 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2017-AVI-145 : Vulnérabilités dans Microsoft Skype for Business 2016
- CERTFR-2017-AVI-146 : Vulnérabilité dans Microsoft .NET Framework
- CERTFR-2017-AVI-147 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2017-AVI-148 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2017-AVI-149 : Multiples vulnérabilités dans Windows Internet Explorer
- CERTFR-2017-AVI-150 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2017-AVI-151 : Vulnérabilité dans Microsoft Malware Protection Engine
- CERTFR-2017-AVI-152 : Multiples vulnérabilités dans Cisco WebEx Meetings Server

Gestion détaillée du document

15 mai 2017 version initiale.