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 mars 2016
N° CERTFR-2016-ACT-011

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2016-ACT-011

1 - Mise à jour mensuelle de Microsoft

Le 08 mars, lors de sa mise à jour mensuelle, Microsoft a publié treize bulletins de sécurité, dont cinq considérés critiques et huit importants :

- MS16-023 (critique) concernant Internet Explorer ;
- MS16-024 (critique) concernant le navigateur Edge ;
- MS16-026 (critique) concernant les polices de caractères de type Opentype ;
- MS16-027 (critique) concernant Windows Media ;
- MS16-028 (critique) concernant la bibliothèque PDF dans Windows ;
- MS16-025 (important) concernant le chargement des bibliothèques dans Windows ;
- MS16-030 (important) concernant Windows OLE ;
- MS16-031 (important) concernant Microsoft Windows ;
- MS16-032 (important) concernant le service d'authentification secondaire de Windows ;
- MS16-033 (important) concernant le pilote de stockage de masse USB de Windows ;
- MS16-034 (important) concernant le noyau de Windows ;
- MS16-029 (important) concernant Microsoft Office ;
- MS16-035 (important) concernant le cadriciel .NET.

Navigateurs

Cette mise à jour corrige treize vulnérabilités dans Internet Explorer qui permettent toutes une exécution de code à distance. Cinq d'entre elles sont également présentes dans le navigateur Edge, à savoir les vulnérabilités CVE-2016-0102, CVE-2016-0105, CVE-2016-0109, CVE-2016-0110 et CVE-2016-0111.

Le navigateur Edge est également concerné par six autres vulnérabilités spécifiques, dont cinq permettent d'exécuter du code arbitraire lors d'une visite d'un site malveillant. La dernière vulnérabilité concerne une possible fuite d'informations, rendue possible par un défaut au niveau de la gestion de la politique de référent ("referrer policy"), pouvant déboucher sur la révélation du contexte d'une requête ou sur l'historique de navigation d'un utilisateur.

Bureautique

Deux vulnérabilités critiques de type corruption de mémoire ont également été corrigées dans Microsoft Office. Celles-ci sont susceptibles de permettre une exécution de code à distance lors de l'ouverture d'un fichier spécialement conçu.

La vulnérabilité CVE-2016-0057 touche également la suite de logiciels de bureautique et est causée par la présence d'un binaire comportant une signature numérique invalide. Un attaquant pourrait ainsi remplacer ce binaire par un code malveillant, la suite Office ne pouvant pas distinguer le fichier original de celui modifié en se basant sur la signature . La vulnérabilité a été corrigée en fournissant un binaire correctement signé.

Windows

La bibliothèque de gestion des polices OpenType dans Windows a bénéficié de deux correctifs. Le premier concerne la vulnérabilité CVE-2016-0121 couvrant une corruption de mémoire lors de l'analyse syntaxique de certaines polices de caractères et pouvant permettre une exécution de code arbitraire. La seconde vulnérabilité est similaire mais n'a pour conséquence potentielle qu'un déni de service.

Les vulnérabilités CVE-2016-0098 et CVE-2016-0101 touchent Windows Media et sont jugées critiques car permettant une exécution du code à distance en intégrant du contenu multimédia malveillant dans une page Internet ou bien encore dans un courrier électronique.

Les deux dernières vulnérabilités critiques (CVE-2016-0117 et CVE-2016-0118), si elles sont exploitées, peuvent également conduire à une exécution de code à distance lorsqu'un utilisateur ouvre un fichier PDF piégé.

D'autres vulnérabilités de Windows permettant une exécution de code ont également été corrigées : celles-ci sont jugées par Microsoft comme importantes et non critiques en raison de leur difficulté d'exploitation. Deux d'entre elles concernent OLE au niveau de la validation des entrées utilisateurs, une autre est causée par un manque de validation lors du chargement de certaines bibliothèques. Cette dernière oblige cependant l'attaquant à obtenir un accès local préalablement à l'exploitation de la vulnérabilité.

Les sept dernières vulnérabilités peuvent permettre de déclencher des élévations de privilèges. A noter que l'une d'elles est liée au pilote USB de Windows, le CERT-FR en profite donc pour rappeler qu'il convient de toujours traiter les supports de stockage de masse amovibles avec prudence, voire la plus grande méfiance lorsque ceux-ci proviennent d'une origine inconnue. En effet, ceux-ci sont encore le vecteur d'attaque de prédilection pour la pénétration des réseaux non connectés à Internet.

Pour finir, le cadriciel .NET reçoit également un correctif car l'un de ses composants ne valide pas correctement certains éléments de documents XML signés, ce qui pourrait compromettre l'intégrité de ceux-ci et la confiance placée en la signature.

Recommandations

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

Documentation

- Avis CERTFR-2016-AVI-087
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-087
- Avis CERTFR-2016-AVI-088
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-088
- Avis CERTFR-2016-AVI-089
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-089
- Avis CERTFR-2016-AVI-090
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-090
- Avis CERTFR-2016-AVI-091
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-091

2 - Rappel des avis émis

Dans la période du 07 au 13 mars 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-082 : Multiples vulnérabilités dans le noyau Linux de Debian
- CERTFR-2016-AVI-083 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-084 : Multiples vulnérabilités dans Samba
- CERTFR-2016-AVI-085 : Multiples vulnérabilités dans les produits Adobe
- CERTFR-2016-AVI-086 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-087 : Multiples vulnérabilités dans Microsoft Internet Explorer
- CERTFR-2016-AVI-088 : Multiples vulnérabilités dans Microsoft Edge
- CERTFR-2016-AVI-089 : Multiples vulnérabilités dans Microsoft Windows
- CERTFR-2016-AVI-090 : Multiples vulnérabilités dans Microsoft Office
- CERTFR-2016-AVI-091 : Vulnérabilité dans Microsoft .NET Framework

- CERTFR-2016-AVI-092 : Multiples vulnérabilités dans Google Chrome
- CERTFR-2016-AVI-093 : Multiples vulnérabilités dans les produits Cisco
- CERTFR-2016-AVI-094 : Multiples vulnérabilités dans Adobe Flash Player
- CERTFR-2016-AVI-095 : Vulnérabilité dans Citrix License Server
- CERTFR-2016-AVI-096 : Multiples vulnérabilités dans SPIP

Gestion détaillée du document

14 mars 2016 version initiale.