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 12 avril 2017
N° CERTFR-2017-ALE-007

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Microsoft Office

Gestion du document

Référence	CERTFR-2017-ALE-007
Titre	Vulnérabilité dans Microsoft Office
Date de la première version	10 avril 2017
Date de la dernière version	12 avril 2017
Source(s)	Article de blogue McAfee du 07 avril 2017
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

– exécution de code arbitraire

2 - Systèmes affectés

Microsoft Office toutes versions

3 - Résumé

Une vulnérabilité a été découverte dans *Microsoft Office*. Elle permet à un attaquant de provoquer une exécution de code arbitraire.

La vulnérabilité exploitée est déclenchée lors de l'ouverture d'un document Microsoft Word contenant un objet OLE2link. Le processus winword.exe effectue alors une requête HTTP vers un serveur de l'attaquant pour télécharger un fichier au format HTA contenant un script malveillant qui sera ensuite exécuté. D'après les observations de FireEye (cf. documentation), le script termine le processus winword.exe et affiche un document Word factice à l'attention de l'utilisateur. Le script semble aussi pouvoir télécharger des charges malveillantes additionnelles.

On notera cependant que la protection *Protected View* de Microsoft Office, activée par défaut pour les versions 2013 et 2016, permet d'empêcher l'exécution des fonctionnalités malveillantes du document. Il convient alors de s'assurer que cette fonctionnalité est bien active.

Le CERT-FR recommande une attention particulière à la réception de courriel non sollicité et de ne pas ouvrir les documents attachées à de tels messages. De façon générale, la plus grande prudence est conseillée face à toutes pièces jointes suspectes.

À l'occasion de la mise à jour de sécurité du mois d'avril 2017, cette vulnérabilité a été corrigée par Microsoft.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Microsoft du 11 avril 2017
  https://portal.msrc.microsoft.com/fr-fr/security-guidance/releasenotedetail/42b8fa28-9d09-e711-80d9-000d3a32fc99
- Avis CERT-FR CERTFR-2017-AVI-108 Multiples vulnérabilités dans Microsoft Office
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-108
- Article de blogue McAfee du 07 avril 2017
  https://securingtomorrow.mcafee.com/mcafee-labs/critical-office-zero-day-attacks-detected-wild/
- Article de blogue FireEye du 8 avril 2017
  https://www.fireeye.com/blog/threat-research/2017/04/acknowledgement_ofa.html

Gestion détaillée du document

10 avril 2017 version initiale.
12 avril 2017 clôture de l'alerte.