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 mars 2017
N° CERTFR-2017-ALE-002

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Microsoft Windows

Gestion du document

Référence	CERTFR-2017-ALE-002
Titre	Vulnérabilité dans Microsoft Windows
Date de la première version	20 février 2017
Date de la dernière version	15 mars 2017
Source(s)	Rapport de Bogue de Project Zero du 16 février 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)

- atteinte à la confidentialité des données

2 - Systèmes affectés

- Windows Vista
- Windows 7
- Windows 8.1
- Windows 10

3 - Résumé

Une vulnérabilité a été découverte dans *Microsoft Windows*. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données.

La vulnérabilité présente dans la bibliothèque Graphics Device Interface (*gdi32.dll*) de Windows permet à un attaquant de lire des portions de mémoire auquel il n'a pas normalement accès.
Cette faille provient d'un manque de vérification dans la gestion des Device Independant Bitmaps (DIB) qui sont contenus dans les fichiers de type Enhanced Metafiles (EMF).

L'attaque peut être déclenchée si un utilisateur se rend sur un site internet contenant un fichier *.emf* piégé en utilisant Internet Explorer.

Un fichier *.emf* peut également être inclus dans d'autres documents (ex. *.docx*), ce qui augmente la surface d'attaque. Le chercheur Mateusz Jurczyk dit avoir réussi à exploiter la vulnérabilité à distance par le biais de *Office Online*.

L'impact de cette vulnérabilité dépend de l'emplacement où est chargé le fichier malveillant en mémoire, et de ce qui est disponible dans les adresses proches.

À l'occasion de la mise à jour de sécurité du mois de mars 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 MS17-013 du 14 mars 2017
  https://technet.microsoft.com/fr-fr/library/security/MS17-013
- Avis CERT-FR CERTFR-2017-AVI-082 Multiples vulnérabilités dans Microsoft Windows
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-082
- Rapport de Bogue de Project Zero du 16 février 2017
  https://bugs.chromium.org/p/project-zero/issues/detail?id=992
- Référence CVE CVE-2017-0038
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0038

Gestion détaillée du document

20 février 2017 version initiale.
15 mars 2017 clôture de l'alerte