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 11 mai 2017
N° CERTFR-2017-ALE-009

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Microsoft Malware Protection Engine

Gestion du document

Référence	CERTFR-2017-ALE-009
Titre	Vulnérabilité dans Microsoft Malware Protection Engine
Date de la première version	09 mai 2017
Date de la dernière version	15 mai 2017
Source(s)	Bulletin de sécurité Microsoft 4022344 du 08 mai 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 à distance

2 - Systèmes affectés

- Microsoft Forefront Endpoint Protection 2010
- Microsoft Endpoint Protection
- Microsoft Forefront Security pour SharePoint Service Pack 3
- Microsoft System Center Endpoint Protection
- Microsoft Security Essentials
- Windows Defender pour Windows 7
- Windows Defender pour Windows 8.1
- Windows Defender pour Windows RT 8.1
- Windows Defender pour Windows 10, Windows 10 1511, Windows 10 1607, Windows Server 2016, Windows 10 1703
- Windows Intune Endpoint Protection

3 - Résumé

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

4 - Description

Les chercheurs Natalie Silvanovich et Tavis Ormandy de Google Project Zero ont révélé l'existence d'une vulnérabilité dans le Malware Protection Engine de Microsoft (cf. section Documentation). Celui-ci est le moteur de nombreux produits de sécurité Microsoft.

Cette vulnérabilité est particulièrement critique car elle est présente par défaut dans toutes les dernières versions de Windows et permet une exécution de code à distance avec les privilèges `System`. De plus, cette vulnérabilité est déclenchée dès qu'un fichier malveillant est balayé par le Malware Protection Engine. Plus concrètement, il suffit uniquement de recevoir un courriel piégé ou de se rendre sur un site malveillant pour risquer une infection.

Toutefois, le 8 mai 2017, Microsoft a annoncé la sortie d'un correctif de sécurité (cf. section Documentation) à l'occasion de sa mise à jour mensuelle. De plus, les systèmes devraient se mettre à jour automatiquement à partir du moment où cette option n'est pas désactivée. Microsoft a également annoncé que cette mise à jour devrait être intégralement déployée sous 48 heures.

Le CERT-FR recommande donc de vérifier que le correctif est bien installé (cf. section Documentation), ou le cas échéant, de mettre ses sytèmes à jour dans les plus brefs délais.

5 - Solution

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

6 - Documentation

- Avis CERT-FR CERTFR-2017-AVI-151
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-151/index.html
- Bulletin de sécurité Microsoft 4022344 du 08 mai 2017
  https://technet.microsoft.com/en-us/library/security/4022344.aspx
- Google Project Zero
  https://bugs.chromium.org/p/project-zero/issues/detail?id=1252&desc=5
- Support Microsoft
  https://support.microsoft.com/en-us/help/2510781/microsoft-malware-protection-engine-deployment-information
- Référence CVE CVE-2017-0290
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0290

Gestion détaillée du document

09 mai 2017 version initiale.

10 mai 2017 ajout du lien vers l'avis CERT-FR CERTFR-2017-AVI-151.

15 mai 2017 clôture de l'alerte.