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 02 novembre 2016
N° CERTFR-2016-ALE-008

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans Microsoft Windows

Gestion du document

Référence	CERTFR-2016-ALE-008
Titre	Vulnérabilité dans Microsoft Windows
Date de la première version	02 novembre 2016
Date de la dernière version	09 novembre 2016
Source(s)	Annonce Microsoft du 01 novembre 2016
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)

– élévation de privilèges

2 - Systèmes affectés

Microsoft Windows, toutes versions

3 - Résumé

Une vulnérabilité a été découverte dans *Microsoft Windows*. Elle permet à un attaquant de provoquer une élévation de privilèges.

4 - Description

Le 31 octobre 2016, le groupe d'analyse de la menace de Google (Threat Analysis Group) a annoncé publiquement l'existence d'une vulnérabilité de type 0 jour permettant une élévation de privilèges dans le noyau de Windows (cf. section Documentation).
Celle-ci est activement exploitée, dans le cadre d'attaques ciblées, de manière conjointe avec la vulnérabilité CVE-2016-7855 affectant le Flash Player d'Adobe (cf. section Documentation).
Microsoft a publié un correctif le 8 novembre 2016, à l'occasion de leur mise à jour mensuelle.

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-2016-AVI-374 Microsoft Windows
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-374/index.html
- Référence CVE CVE-2016-7255
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7255
- Annonce Microsoft du 01 novembre 2016
  https://blogs.technet.microsoft.com/mmpc/2016/11/01/our-commitment-to-our-customers-security/
- Google Security Blog
  https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html
- Avis CERT-FR CERTFR-2016-AVI-364 Adobe Flash Player
  http://www.cert.ssi.gouv.fr/site/CERTFR-2016-AVI-364/index.html
- Microsoft Device Guard
  https://technet.microsoft.com/en-us/itpro/windows/keep-secure/introduction-to-device-guard-virtualization-based-security-and-code-integrity-policies

Gestion détaillée du document

02 novembre 2016 version initiale.

09 novembre 2016 clôture de l'alerte.