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-003

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Vulnérabilité dans les navigateurs Microsoft

Gestion du document

Référence	CERTFR-2017-ALE-003
Titre	Vulnérabilité dans les navigateurs Microsoft
Date de la première version	27 février 2017
Date de la dernière version	15 mars 2017
Source(s)	Rapport de Bogue de Project Zero du 23 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)

- exécution de code arbitraire à distance

2 - Systèmes affectés

- Internet Explorer 11 pour Windows 7
- Internet Explorer 11 pour Windows 8.1
- Internet Explorer 11 pour Windows 10
- Internet Explorer 11 pour Windows Server 2012 et 2016
- Microsoft Edge pour Windows 10

3 - Résumé

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

Cette vulnérabilité exploite une faille de type confusion de type et peut être déclenchée en définissant des valeurs particulières pour les propriétés d'un objet tableau dans une page Web spécialement conçue.

On notera que cette vulnérabilité est atténuée par l'utilisation de la mesure de sécurité de Windows *Control Flow Guard* (CFG) au sein de l'application. Un attaquant souhaitant exploiter la vulnérabilité devra ainsi mettre en oeuvre un contournement de la contre-mesure CFG.

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 MS17-006 du 14 mars 2017
  https://technet.microsoft.com/fr-fr/library/security/MS17-006
- Avis CERT-FR CERTFR-2017-AVI-079 Multiples vulnérabilités dans Microsoft Internet Explorer
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-079
- Avis CERT-FR CERTFR-2017-AVI-080 Multiples vulnérabilités dans Microsoft Edge
  http://www.cert.ssi.gouv.fr/site/CERTFR-2017-AVI-080
- Rapport de Bogue de Project Zero du 23 février 2017
  https://bugs.chromium.org/p/project-zero/issues/detail?id=1011
- Référence CVE CVE-2017-0037
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0037

Gestion détaillée du document

27 février 2017 version initiale.

28 février 2017 mise à jour des systèmes affectés.

15 mars 2017 clôture de l'alerte

Conditions d'utilisation de ce document :	`http://cert.ssi.gouv.fr/cert-fr/apropos.html`
Dernière version de ce document :	`http://cert.ssi.gouv.fr/site/CERTFR-2017-ALE-003`