

Alerte : Nouvelle vulnérabilité dans les navigateurs Microsoft



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

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.

4 – Contournement provisoire

Une vulnérabilité présente dans les navigateurs Internet Explorer et Edge permet à un attaquant d'exécuter du code arbitraire depuis une page internet malveillante.

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.

Aucun correctif n'est prévu par Microsoft avant la publication mensuelle des correctifs de sécurité du mois de mars. Dans l'attente de la disponibilité d'un correctif de sécurité, le CERT-FR recommande de privilégier l'utilisation de navigateurs autres qu'Internet Explorer ou Edge pour la navigation sur Internet.

5 – Documentation

- 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>

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIEF n°93 84 03041 84)
- Formation de C.I.L.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Vulnérabilité dans les navigateurs Microsoft*