

Edge est affectée par une faille que Microsoft s'abstient de corriger

Des chercheurs de **Talos**, la filiale sécurité de Cisco, ont découvert une vulnérabilité critique affectant Edge, le navigateur Internet de Microsoft dédié à Windows 10.

Mais, plus de 8 mois après la transmission des informations ad hoc, la brèche de sécurité relative au browser n'est pas colmatée.

Pourtant, « *une page Web spécialement conçue peut entraîner un contournement du système de sécurité du contenu (Content Security Policy ou CSP, NDLR), avec pour résultat une fuite d'information* », avance Nicolai Grødum, Technical Leader chez Cisco dans son [alerte](#).

Le mécanisme CSP permet au développeur de configurer les entêtes HTTP et informer le navigateur exploité par les visiteurs des ressources dont ils peuvent bénéficier (Javascript, CSS...).

En contournant ces CSP, un attaquant peut donc charger un code Javascript malicieux sur un site distant et effectuer des opérations intrusives telles que la collecte d'informations à partir des cookies des utilisateurs ou l'enregistrement des frappes dans les formulaires de la page.

Des millions d'internautes concernés

Le problème vient du chargement de la page « about:blank » (une page vierge) dont les restrictions en matière de règles de protection des contenus ont été levées dans la navigateur Edge. « *En chargeant un nouveau document à l'aide de window.open (« », « _ blank ») et avec document.write-in (about:blank) un attaquant peut contourner les restrictions CSP sur le document et le code Javascript de la page d'origine et rejoindre d'autres sites, souligne le chercheur qui ajoute que un attaquant peut créer une page Web malveillante pour déclencher cette vulnérabilité.* »

La vulnérabilité est absente de Firefox, précise Nicolai Grødum. Et elle a été corrigée pour Safari et Chrome. La faille y était référencée CVE-2017-2419 et CVE-2017-2419 respectivement.

Selon NetMarketShare, Edge composait 5,66% du marché des navigateurs en août dernier. Autrement dit, des millions d'utilisateurs dans le monde naviguent à risque.

On ignore en l'état actuel pourquoi Microsoft s'abstient de colmater cette brèche sur son propre navigateur.

Lire également

[Navigateurs Web : les meilleurs sur PC et sur mobile](#)

[Patch Tuesday : un été chargé en vulnérabilités critiques](#)

[Edge, invité d'honneur de la dernière Build de Windows 10](#)