

Internet Explorer : une faille zero day via les fichiers .MHT ?

Même si l'on ne s'en sert jamais, la simple présence d'[Internet Explorer](#) sur un ordinateur sous Windows offre un point d'entrée pour une attaque malveillante.

C'est ce qu'affirme le chercheur en sécurité John Page qui a révélé l'existence d'une faille zero-day dans le navigateur Microsoft grâce à laquelle il serait possible de dérober des données depuis un système Windows.

Vulnérabilités sur les fichiers .MHT

La vulnérabilité se situe au niveau des fichiers de type MHT, le standard avec lequel toutes les versions d'Internet Explorer sauvegardent les pages web lorsqu'un internaute les enregistre. Les navigateurs Web actuels n'utilisent pas le format .MHT et lorsqu'un utilisateur tente d'accéder à ce fichier, Windows ouvre IE par défaut.

Il suffirait alors à un pirate d'inciter sa victime à ouvrir un fichier .MHT sous forme de fichier joint pour pouvoir injecter un code malveillant.

John Page a créé une preuve de concept et indique qu'il a [testé](#) l'exploit sur la dernière version du navigateur Internet Explorer 11 sur Windows 7, Windows 10 et Windows Server 2012 R2.

Pas de correctif d'urgence prévu par Microsoft

Le chercheur explique avoir informé Microsoft de la situation le 27 mars qui n'a pas considéré que ce bug méritait un correctif en urgence.

"Nous avons décidé qu'une solution à ce problème serait envisagée dans une future version de ce produit ou service", aurait déclaré l'éditeur. « Pour l'instant, nous ne fournirons pas de mises à jour régulières sur l'état d'avancement de ce problème, et nous avons clos cette affaire. »

John Page a alors décidé de rendre publique sa découverte.