Internet Explorer en alerte d'une nouvelle vulnérabilité «zero day»

Et une de plus! Microsoft a émis, vendredi 28 janvier, une nouvelle alerte de sécurité visant une faille dites « zero day » d'Internet Explorer, autrement dit publique et exploitatble. L'éditeur de Redmond déclare néanmoins *« ne disposer d'aucune information sur l'exploitation effective de cette vulnérabilité »*. La vigilance ne s'en impose pas moins.

La brèche permet de mener des attaques de type *cross-site scripting* (XSS) en autorisant l'exécution de script malveillant sur le poste client depuis une page web infectieuse. *« La vulnérabilité provient de la manière dont le MHTML interprète les requêtes au format MIME pour les blocs de contenu dans un document*, explique Microsoft. *Il est possible que sous certaines conditions cette vulnérabilité permette à un attaquant d'injecter un script côté client dans la réponse d'une requête Web s'exécutant dans l'environnement client d'Internet Explorer. »* Le format MHTML (*MIME Encapsulation of Aggregate Documents, such as HTML*) permet d'enregistrer et envoyer un fichier HTML avec les éléments externes (images, scripts…) à la page web.

Fermer le protocole MHTML

Toutes les versions de Windows, poste de travail et serveurs, sont affectées (à l'exception de Windows Server 2008 et son successeur R2 quand ils sont installés avec l'option *Server Core*). Si Internet Explorer, qui supporte le MHTML depuis sa version 6, est principalement affecté, la question se pose aussi pour le navigateur Opera également compatible avec le protocole.

Pour l'heure et par définition, il n'existe aucun correctif pour se prémunir de telles attaques. Redmond déclare travailler activement à ce problème avec ses partenaires de son *Active Protections Program*, notamment pour limiter les attaques potentielles en sécurisant les systèmes côté serveurs. Les attaquants devront néanmoins convaincre leurs victimes de visiter les pages infectieuses. En attendant ce correctif (qui, en regard de la proximité du prochain bulletin de sécurité le 8 février, pourrait ne pas arriver avant mars prochain), Microsoft recommande de fermer le protocole MHTML. L'éditeur a également ouvert un blog dédié à la question. A suivre en attendant le correctif adéquat.