Internet Explorer bientôt victime des pirates chinois?

Une faille critique non corrigée frappe Internet Explorer. Pas celle révélée en fin d'année par Microsoft. Une nouvelle vulnérabilité sur laquelle **l'éditeur de Redmond a plus ou moins fermé les yeux**. Ce qui est d'autant plus inquiétant que la brèche en question aurait été repérée, notamment du côté de la Chine.

C'est en tout cas ce que déclare **Michal Zalewski** à notre confrère américain *ComputerWorld*. *« J'ai des raisons de croire que la vulnérabilité évidemment exploitable [dans IE] détectable par cross_fuzz est indépendamment connue par des tiers en Chine »*, déclare le développeur de chez Google. Il travaille notamment sur le moteur de rendu WebKit qui équipe Chrome et Safari, et a programmé un outil de *« cross fuzzing »* permettant d'automatiser la recherche de failles dans le code des applications. Or, le fichier de résultats d'analyse msie_crash.txt aurait « accidentellement » fuité avant de se retrouver indexé par le moteur de recherche de Google.

Si jusqu'à présent aucun élément ne permettait de remonter à la source du bug, ce n'est apparemment plus le cas. *« Le 30 décembre*, précise le développeur, *j'ai reçu les recherches suivantes à partir d'une adresse IP en Chine, qui correspondait à des mots-clés mentionnés dans l'un des fichiers cross_fuzz indexés. »* Et de détailler en ligne les requêtes en question qui se concentrent sur **les fonctions de Mshtml.dll**, le moteur d'IE.

Cela n'aurait rien de dramatique si Microsoft avait réagi plus tôt. Michal Zalewski a en effet alerté l'éditeur de Windows dès juillet dernier de l'existence des failles, comme il l'a fait pour les autres acteurs, Mozilla Firefox, Opera et Apple Safari qui ont, en parti, corrigé les erreurs sur la base des découvertes du développeur. **Les équipes de Microsoft argumentaient qu'elles n'avaient pas réussi à reproduire le bug**, jusqu'à ce qu'elles y parviennent… le 29 décembre. Résultat, IE met ses utilisateurs à la merci des pirates (chinois ou non). Reste à savoir combien de temps il faudra pour que la faille en question soit exploitée… et corrigée.