

4 failles zero day dans IE publiées, que fait Microsoft ?

La liste commence à être longue en matière de zero day pour Microsoft. Après la correction en urgence d'une faille critique touchant l'ensemble des versions de Windows, c'est au tour d'Internet Explorer d'être visé non pas par une, mais par 4 vulnérabilités critiques non corrigées.

Elles ont été découvertes par les équipes de Zero Day Initiative de HP, il y a plus de 120 jours. C'est le temps normalement laissé à Microsoft pour corriger les erreurs avant d'en publier les détails. Oui mais voilà la firme de Redmond a un peu traîné la patte en demandant des délais supplémentaires qui lui ont été accordés. Mais après plus de 6 mois (les vulnérabilités ont été montrées lors de Pwn2wn le 12 novembre 2014), [ZDI a décidé de brusquer les choses](#) et vient de publier les 4 failles zero day qui touchent IE. La firme a donc émis 4 bulletins [ZDI-15-359](#), [ZDI-15-360](#), [ZDI-15-361](#) et [ZDI-15-362](#).

Une exploitation encore lointaine

Les 4 failles présentent un risque d'exécution de code à distance. Elles touchent différents composants présents dans IE comme les objets CattrArray, CTableLayout, CCurrentStyle ou CTreePos.

Les experts en sécurité se veulent néanmoins rassurant en estimant que les chances sont faibles de trouver bientôt des exploits utilisant ces brèches. Pour [Wolfgang Kandek, CTO de Qualys](#), « *il est difficile de faire de l'ingénierie inversé sur ces failles, car les détails sont relativement rares* ». Il n'empêche cette publication intervient dans un contexte tendu en matière de sécurité. La semaine dernière, Microsoft a publié un Patch Tuesday costaud corrigeant notamment une faille critique issue du piratage de Hacking Team.

A lire aussi :

[Microsoft soigne la sécurité de son navigateur web Internet Explorer](#)

[Microsoft renforce l'utilisation du HTTPS au sein d'Internet Explorer](#)

© Maxx-Studio – Shutterstock