Microsoft et Google en passe de débrancher SSL 3.0 des navigateurs

Il y a quelques semaines, des chercheurs de Google ont découvert une faille dans SSL 3.0, un protocole de chiffrement très employés dans les navigateurs et les sites web, qui date de près de 18 ans. La vulnérabilité en question peut permettre à un assaillant de dérober des mots de passe et les cookies d'un navigateur et elle passe par une attaque de type « man-in-the-middle », l'attaquant devant s'interposer entre le site web et le navigateur ciblé. Les chercheurs ont nommé ce bogue sous l'acronyme Poddle (Padding Oracle On Downgraded Legacy Encryption).

Or pour éviter l'utilisation de cette faille, le meilleur remède est de désactiver SSL 3.0. Plusieurs grands noms du web se sont penchés sur la question. Apple a été un des premiers à dégainer en corrigeant rapidement Safari de cette faille. Aujourd'hui, Microsoft et Google suivent en annonçant dans un premier temps une méthode pour désactiver SSL 3.0. La firme de Redmond propose un utilitaire FixIT pour désactiver automatiquement le protocole concerné sur différentes versions d'IE (y compris IE6). L'éditeur a souligné que SSL 3.0 sera désactivé par défaut dans les prochaines moutures du navigateur. A partir du 1er décembre prochain, Microsoft prévoit d'étendre cette suspension à d'autres services en ligne comme Office 365 et Azure.

Même état d'esprit chez Google qui a annoncé la désactivation de SSL 3.0 dans Chrome 39. La suspension totale interviendra dans la version Chrome 40. La firme de Mountain View a suivi un autre acteur la Fondation Mozilla qui a annoncé une initiative similaire pour Firefox 34 qui sortira le 25 novembre prochain. Au final, Poddle aura signé la fin de SSL 3.0 après près de 20 ans de bons et loyaux services.

A lire aussi :

159 failles corrigées dans le navigateur web Google Chrome !
Plus de 100 000 sites en SSL RSA 1024 bits écartés des navigateur