# Covid-19 : quand l'accessibilité du web prime sur la sécurité

Malgré leurs fragilités, TLS 1.0 et 1.1 vivront un peu plus longtemps que prévu dans les navigateurs web.

Ces deux versions du protocole, publiées en 1999 et en 2006, sont aujourd'hui considérées comme obsolètes. Notamment parce qu'elles exploitent des algorithmes de chiffrement (MD5 et SHA-1) dont la sécurité a été mise à mal.

En octobre 2018, Apple, Google, Microsoft et Mozilla avaient conjointement annoncé leur intention de désactiver la prise en charge desdites versions dans leurs butineurs.

Apple et Mozilla avaient fixé l'échéance à mars 2020. Même chose pour Google, qui affirmait prévoir une exception jusqu'en janvier 2021 pour les entreprises.

Microsoft évoquait quant à lui le premier semestre 2020. Et ne parlait pas d'une suppression, mais d'une « désactivation par défaut ».

Il en est toujours question, mais cela n'interviendra pas avant le passage d'Edge 84 sur le canal stable. C'est-à-dire en juillet prochain. La prise en charge de TLS 1.0 et 1.1 sera même maintenue jusqu'au 8 septembre sur Internet Explorer 11 et sur la version « originale » d'Edge.

Microsoft explique avoir pris cette décision « compte tenu de la conjoncture mondiale ».

Le discours de Mozilla va dans le même sens. L'actualisation des notes de version de Firefox 74 (lancé le 10 mars) en témoigne. La fondation déclare avoir retiré, pour une durée indéterminée, la fonctionnalité qui déclenchait une erreur sur les sites n'utilisant pas au moins TLS 1.2. Officiellement, il s'agit de favoriser l'accès aux sites gouvernementaux « critiques » qui diffusent de l'info Covid-19.

Chez Google, la fin de TLS 1.0 et 1.1 dans Chrome ne prendra pas effet avant le passage de la version 83 sur le canal stable. Date prévue : le 19 mai 2020.

Au dernier pointage de Qualys, 97,5 % des sites prennent en charge TLS 1.2 (publié en 2008) ; 28 %, TLS 1.3 (finalisé en 2018).

## Chrome : les cookies tiers passeront le printemps

Google prend une autre mesure au nom de la stabilité du web pendant la crise sanitaire.

Elle consiste à éliminer temporairement les stratégies de cookies qui ont commencé à s'appliquer en février avec Chrome 80.

Ces dernières s'appuient sur le paramètre SameSite pour resserrer l'étau sur les usages dans contextes tiers.

Censées renforcer la sécurité, elles peuvent néanmoins perturber certains services, entre autres d'authentification.

Dans ce contexte, Google préfère reporter leur mise en œuvre à cet été. Objectif : ne pas menacer l'accès à des sites « essentiels » (banque, alimentation, santé, pouvoirs publics).

*Photo d'illustration ©*