RFC 9852 : New Protocols Using TLS Must Require TLS 1.3

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 juillet 2026

Date de publication du RFC : Juillet 2026

https://www.bortzmeyer.org/9852.html

Si vous concevez des protocoles réseau utilisant la cryptographie, vous utiliserez souvent TLS. Dans ce cas, pour un nouveau protocole, n'ayant pas à gérer l'existant, l'IETF vous conseille fortement, dans ce RFC, d'exiger dans la définition du protocole qu'il faut au moins la version 1.3 de TLS.

TLS 1.3 (RFC 9846 [1]) est largement déployé (vous trouverez difficilement un serveur Internet qui n'ait que la version précédente, la 1.2, normalisée dans le RFC 5246), a de meilleures preuves de sécurité, et protège mieux. Il est donc raisonnable de le définir comme version minimum. Attention, ce RFC est destiné aux gens qui conçoivent des protocoles réseau, par exemple à l'IETF, pas à l'administrateur réseaux de terrain. Celui-ci ou celle-ci peut continuer à utiliser TLS 1.2.

La section 6 de notre RFC détaille les faiblesses de TLS 1.2, en remarquant qu'on peut configurer TLS 1.2 de manière sûre (couper la renégociation <https://www.bortzmeyer.org/tls-renego.html>, désactiver les algorithmes de cryptographie faibles, etc) mais que ce n'est pas toujours fait en pratique. Et bien des failles de sécurité ont frappé 1.2, alors que 1.3 n'y était pas vulnérable (on parle bien d'une faille du protocole, pas d'un programme particulier mettant en œuvre ce protocole). C'était par exemple le cas de Beast <https://www.bortzmeyer.org/beast-tls.html>.

Certains protocoles ont déjà pris cette décision d'exiger TLS 1.3, par exemple QUIC (RFC 9001), qui impose de couper tout de suite la connexion si l'autre partie ne fait pas de 1.3. D'autres n'ont pas encore sauté le pas, ainsi, DoT (RFC 8310) permet encore TLS 1.2. Notez que le RFC 9325, que notre RFC met à jour, ne donnait TLS 1.3 que comme « recommandé » (section 5).

La plupart des bibliothèques TLS permettent au programmeur d'imposer une version minimale de TLS donc respecter cette exigence « au moins 1.3 » ne devrait pas poser de problème (section 4).

Le RFC note (section 3) qu'à l'heure actuelle, le monde de la cryptographie est occupé à préparer une transition vers des algorithmes post-quantiques (RFC 9958). Comme TLS 1.2 est gelé (cf. RFC 9851), les solutions post-quantiques <https://www.nist.gov/cybersecurity/what-post-quantum-cryptography> n'y seront pas intégrées et, si un CRQC ("*Cryptographically Relevant Quantum Computer*") finit par apparaitre un jour, TLS 1.2 ne sera plus sûr.

Notez enfin que cette exigence d'avoir la version 1.3 s'applique à TLS, mais pas à DTLS.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc9846.txt