RFC 8996 : Deprecating TLSv1.0 and TLSv1.1

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 24 mars 2021. Dernière mise à jour le 25 mars 2021

Date de publication du RFC : Mars 2021

https://www.bortzmeyer.org/8996.html

Ce RFC est très court, car il s'agit juste de formaliser une évidence : les versions 1.0 et 1.1 du protocole de cryptographie TLS ne devraient plus être utilisées, elles souffrent de diverses failles, notamment de sécurité. Les seules versions de TLS à utiliser sont la 1.2 (recommandée depuis 2008 !) et la 1.3 (publiée en 2018). Ainsi, une bibliothèque TLS pourra retirer tout le code correspondant à ces versions abandonnées, ce qui diminuera les risques (moins de code, moins de bogues).

Que reproche-t-on exactement à ces vieux protocoles (section 1 du RFC) ?

— Ils utilisent des algorithmes de cryptographie dépassés et dangereux, par exemple TLS 1.0 impose de gérer Triple DES, et SHA-1 est utilisé à plusieurs endroits. Un des points les plus problématiques à propos des vieilles versions de TLS est en effet leur dépendance vis-à-vis de cet algorithme de condensation SHA-1. Celui-ci est connu comme vulnérable <https://sha-mbles.github.io/>.
— Ils ne permettent pas d'utiliser les algorithmes modernes, notamment le chiffrement intègre.
— Indépendamment des défauts de ces vieux protocoles, le seul fait d'avoir quatre versions à gérer augmente les risques d'erreur, pouvant mener à des attaques par repli.
— Des développeurs de bibliothèques TLS ont manifesté leur souhait de retirer les vieilles versions de TLS, ce qui implique leur abandon officiel par l'IETF.
— Pour davantage de détails sur les faiblesses reprochées aux vieilles versions de TLS, regardez le rapport SP800-52r2 du NIST <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf> ou bien le RFC 7457[1]. S'il existe bien des contournements connus pour certaines de ces vulnérabilités, il est quand même plus simple et plus sûr d'abandonner ces anciennes versions 1.0 et 1.1.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7457.txt

Désormais, la programmeuse ou le programmeur qui veut faire mincir son code en retirant TLS 1.0 et 1.1 peut, si des utilisateurs contestent, s'appuyer sur cette décision de l'IETF. Désormais, la règle est simple : le client ne doit pas proposer TLS 1.0 et 1.1, et s'il le fait le serveur ne doit pas l'accepter. Cela concerne de nombreux RFC, qui mentionnaient 1.0 et 1.1, et tous n'ont pas encore été mis à jour. Ainsi, le RFC 7562 est toujours d'actualité, simplement la mention qu'il fait de TLS 1.1 est réputée supprimée. De même, le RFC 7525, qui résume les bonnes pratiques d'utilisation de TLS doit désormais se lire en oubliant les quelques endroits où il cite encore TLS 1.1. D'autres RFC avaient déjà été abandonnés, comme par exemple le RFC 5101.

Donc, pour résumer les points pratiques de ce RFC (sections 4 et 5) :

— **N'utilisez pas TLS 1.0.** Le client TLS ne doit pas le proposer dans son `ClientHello`, le serveur TLS ne doit jamais l'accepter.
— **N'utilisez pas TLS 1.1.** Le client TLS ne doit pas le proposer dans son `ClientHello`, le serveur TLS ne doit jamais l'accepter.

Si vous êtes programmeu·r·se, virez le code de TLS 1.0 et 1.1 de vos logiciels. (OpenSSL a prévu de le faire en 2022.) Notez que certains protocoles récents comme Gemini ou DoH (RFC 8484) imposaient déjà TLS 1.2 au minimum.

Comme le note la section 7 du RFC, suivre les recommandations de sécurité exposées ici va affecter l'interopérabilité : on ne pourra plus communiquer avec les vieilles machines. J'ai à la maison une vieille tablette pour laquelle le constructeur ne propose pas de mise à jour logicielle et qui, limitée à TLS 1.0, ne peut d'ores et déjà plus se connecter à beaucoup de sites Web en HTTPS. L'obsolescence programmée en raison de la sécurité. . .Plus grave, des organisations peuvent être coincées avec une vieille version de TLS sur des équipements, par exemple de contrôle industriel, qu'on ne peut pas mettre à jour. (Lors des discussions à l'IETF sur ce RFC, des personnes avaient suggéré d'attendre que le niveau d'utilisation de TLS 1.0 et 1.1 tombe en dessous d'une certaine valeur, avant d'abandonner officiellement ces protocoles. L'IETF a finalement choisi une approche plus volontariste. Mais pensez aux établissements comme les hôpitaux, avec tous les systèmes contrôlés par des vieux PC pas mettables à jour.) Comme toujours en sécurité, il n'y a pas de solution parfaite, uniquement des compromis. Le site de test TLS montre ici un site Web d'une banque qui continue à proposer TLS 1.0 et 1.1, ce qui baisse sa note globale mais est peut-être justifié par le désir de ne pas laisser tomber les clients qui ne peuvent pas facilement changer leur logiciel :

Au contraire, voici ce qu'affiche un Firefox récent quand on essaie de se connecter à un vieux site Web qui n'accepte toujours pas TLS 1.2 :

À noter que DTLS 1.0 (RFC 4347) est également abandonné. Cela laisse DTLS 1.2, le 1.1 n'ayant jamais été normalisé, et le 1.3 n'étant pas prêt à l'époque (il a depuis été publié dans le RFC 9147).

Les RFC 2246 (TLS 1.0) et RFC 4346 (TLS 1.1) ont été officiellement reclassifiés comme n'ayant plus qu'un intérêt historique. Le RFC 7507 est également déclassé, le mécanisme qu'il décrit n'étant utile qu'avec TLS 1.0 et 1.1.