Guide sur le retrait du protocole TLS 1.1

Pour assurer la conformité continue de Moneris[MD] à la norme de l'industrie des cartes de paiement (PCI), **nous retirerons la version 1.1 du protocole de sécurité de la couche de transport (Transport Layer Security ou TLS) en mai 2022**, parce qu'il ne fournit plus un niveau adéquat de protection. De plus, la majorité des navigateurs modernes prennent actuellement en charge des versions plus récentes du protocole, notamment le protocole TLS 1.2 ou un protocole plus récent. Vous trouverez ci-dessous les renseignements de base, les prochaines étapes à suivre et des ressources utiles.

Qu'est-ce que le protocole TLS?

Il s'agit d'un protocole qui assure la confidentialité et l'intégrité des données entre deux applications en communication. TLS est actuellement le protocole de sécurité le plus déployé et il est utilisé pour les navigateurs Web et d'autres applications qui requièrent un échange de données sécurisé par l'entremise d'un réseau. Il fournit une connexion sécurisée à l'utilisateur final à distance grâce au chiffrement et à la vérification de l'identité de l'utilisateur final.

Que devez-vous faire?

Afin d'éviter toute interruption des activités et de prévenir les risques de sécurité, vous devez mettre à jour vos environnements de production et d'assurance de la qualité pour prendre en charge le protocole TLS 1.2 ou un protocole plus récent avant en mai 2022. Heureusement, la prise en charge peut être aussi simple que de recompiler la solution avec des bibliothèques mises à jour ou de mettre à jour un fichier de configuration.

Si vous avez des questions ou si vous avez besoin d'aide, vous pouvez communiquer avec nous à la page Moneris.com/fr-ca/soutien/contact.

Voici quelques ressources utiles :

Bien que le protocole TLS 1.2 puisse être configuré dans une application Web, nous vous recommandons également d'utiliser un serveur Web dont le niveau de sécurité minimum est le protocole TLS 1.2. Consultez ce guide sur la configuration en cliquant ici.

Voici les navigateurs Web qui prennent en charge les protocoles TLS 1.2 et TLS 1.3 :

- Microsoft Windows 10 qui fonctionne avec Microsoft Edge, Internet Explorer 11 ou une version actuelle de Firefox ou de Chrome
- Microsoft Windows 8 qui fonctionne avec Internet Explorer 11 ou une version plus récente, ou une version actuelle de Firefox ou de Chrome
- Mac OS X 11 ou une version plus récente qui fonctionne avec Safari 7 ou une version plus récente, ou une version actuelle de Firefox ou de Chrome

Navigateur	Prise en charge du protocole TLS 1.2 (Cette option n'est pas activée par défaut.)	Cette option est activée par défaut.
Internet Explorer	Version 8	Version 11
Microsoft Edge	-	Toutes les versions
Google Chrome	Version 29	Version 29
Mozilla Firefox	Version 23	Version 27
Safari d'Apple	Version 7	Version 7

Prise en charge du protocole TLS 1.2 par le cadre d'application :

- Pour *Java* : Nous vous recommandons d'utiliser la version *Java 8* ou une version plus récente. La version *Java 7* peut être utilisée, mais elle exige que le protocole TLS 1.2 soit explicitement activé par l'application.
- Pour *.NET* : Nous vous recommandons d'utiliser la version *.NET 4.6* ou une version plus récente. Bien que la version *.NET 4.5* puisse être utilisée, elle exige que le protocole TLS 1.2 soit explicitement activé par l'application. De plus, l'utilisation de *.NET* dépend de la prise en charge du protocole TLS 1.2 par Windows (voir le tableau ci-dessus).
- Pour les applications qui utilisent *OpenSSL* : Nous vous recommandons d'utiliser la version *OpenSSL 1.01* ou une version plus récente.

Validation des demandes

Voici deux façons de vérifier la version de TLS utilisée :

1. **https://www.howsmyssl.com** : Ce site vous fournit une analyse dans sa réponse et il ne requiert pas de traitement JavaScript pour obtenir un résultat. Vous devez recevoir le message de réponse suivant :

   "Your client is using TLS 1.2, the most modern version of the encryption protocol. It gives you access to the fastest, most secure encryption possible on the web."
   (« Votre client utilise le protocole TLS 1.2, qui est la version la plus récente du protocole de chiffrement. Il vous donne accès au chiffrement le plus rapide et le plus sécuritaire sur le Web. »)

2. **SSL Labs** : Ce site vous fournit une liste de toutes les versions et de tous les chiffres de TLS qui sont offerts en tant que serveur ou client.

   Serveur :https://www.ssllabs.com/ssltest/analyze.html?d=account-d.docusign.com

   Client : https://clienttest.ssllabs.com:8443/ssltest/viewMyClient.html