

Points Clés à Retenir sur l'erreur ERR_SSL_UNSUPPORTED_VERSION

Problème	Solution rapide
Version SSL obsolète	Activez ou mettez à jour le protocole TLS dans votre navigateur.
Problèmes avec Firefox	Modifiez les paramètres TLS avec <code>about:config</code> (voir section dédiée).
Problèmes avec Chrome	Vérifiez et activez TLS 1.3 dans <code>chrome://flags</code> .
Certificats SSL invalides	Analysez le certificat SSL avec Qualys SSL Labs .
Impact des extensions	Désactivez les add-ons pouvant perturber les connexions SSL.
Cache et cookies	Effacez les données de navigation pour éviter les interférences.

Résolution de l'erreur ERR_SSL_UNSUPPORTED_VERSION : Guide pas à pas

1. Comprendre les Causes de l'Erreur

L'erreur **ERR_SSL_UNSUPPORTED_VERSION** est souvent due à un protocole SSL ou TLS obsolète utilisé par un site web ou un navigateur. Les versions inférieures à TLS 1.2 sont désormais dépréciées dans la plupart des navigateurs récents, comme Chrome, Firefox, et Edge. Cela peut également signaler :

- Une mauvaise configuration côté serveur.
 - Une connexion utilisant des certificats SSL/TLS invalides.
 - Un navigateur ayant des configurations de sécurité rigides.
-

2. Modifier les Paramètres TLS dans Firefox

Si vous utilisez Firefox, voici la méthode :

1. Ouvrir les réglages avancés :

- Tapez `about:config` dans la barre d'adresse et appuyez sur Entrée.
- Cliquez sur le bouton pour **accepter les risques liés** à la modification des paramètres.

2. Rechercher la clé TLS appropriée :

- Dans la barre de recherche, tapez `security.tls.version.min`.

3. Modifier la version minimale de TLS :

- Double-cliquez pour éditer. Par défaut, ce paramètre est souvent réglé à 3 (TLS 1.2). Diminuez-le à **1 (TLS 1.0)**.

4. Redémarrer Firefox :

- Une fois les changements sauvegardés, redémarrez le navigateur et essayez de visiter à nouveau le site concerné.

⚠ Attention : Réduire la version de TLS peut exposer votre navigateur à des menaces potentielles. Utilisez cette méthode uniquement si vous êtes sûr que le site est sécurisé.

3. Activer ou Mettre à Jour TLS 1.3 dans Chrome

Chrome prend en charge TLS 1.3 par défaut, mais vous pourriez vérifier ou activer manuellement cette option :

1. Accéder aux drapeaux de Chrome :

- Dans la barre d'adresse, saisissez `chrome://flags` et validez.

2. Effectuer une recherche :

- Tapez TLS dans la barre de recherche en haut.

3. Confirmer l'activation de TLS 1.3 :

- Si la fonctionnalité TLS 1.3 est désactivée, activez-la.

4. Redémarrer Chrome :

- Cliquez sur le bouton **Relaunch** pour relancer le navigateur et appliquer les modifications.

À noter : Si l'erreur persiste, essayez d'effacer les paramètres proxy dans Chrome (accessible via `chrome://settings/`).

4. Vérifier l'état des Certificats SSL

Un certificat SSL expiré, mal configuré ou faible peut causer cette erreur. Voici comment analyser rapidement la sécurité d'un site web :

1. Accéder à Qualys SSL Labs :

- Allez sur [Qualys SSL Labs](#) et entrez l'URL du site concerné.

2. Analyser les résultats :

- Vérifiez si le site utilise une version de TLS obsolète, comme TLS 1.0 ou 1.1.

3. Conseil : Si le problème est côté serveur, vous devrez contacter l'administrateur du site pour leur signaler l'erreur.

[Liens d'affiliation connexes pour outils SSL et VPN :_
[NordVPN - Meilleure solution sécurisée](#)

5. Nettoyez les Données de Navigation

Les caches corrompus ou les cookies anciens peuvent également être à l'origine du message d'erreur. Voici les étapes de nettoyage :

1. Ouvrir les paramètres :

- **Chrome** : `chrome://settings/clearBrowserData`.
- **Firefox** : Cliquez sur les trois barres > Paramètres > Vie privée et Sécurité > Cookies et données de sites.

2. Sélectionner les éléments à effacer :

- Cochez les options Cookies et Images et fichiers en cache.

3. Effacer et redémarrer :

- Cliquez sur **Effacer les données** et relancez le navigateur.
-

6. Désactiver les Extensions Non Essentielles

Certaines extensions de navigateur peuvent bloquer les connexions SSL. Désactivez-les temporairement :

1. Désactiver les extensions :

- **Chrome** : chrome://extensions/.
- **Firefox** : Cliquez sur les trois barres > Modules complémentaires > Extensions.

2. Tester le problème après désactivation :

- Rechargez le site après avoir désactivé toutes les extensions et procédez par élimination pour voir si une extension spécifique était la cause.
-

7. Vérifiez l'OS et Vos Drivers

Un système d'exploitation ou des drivers réseau obsolètes peuvent aussi bloquer les connexions sécurisées :

- **Mettez à jour votre système d'exploitation** (Windows, macOS, Linux).
 - **Utilisez un outil de mise à jour automatique des drivers**, comme [EaseUS DriverHandy](#).
-

Foire Aux Questions (FAQ)

1. Que se passe-t-il si "security.tls.version.min" dans Firefox ne fonctionne pas ?

Cela peut se produire si votre version de Firefox est trop ancienne ou si TLS 1.0/1.1 est complètement désactivé. Mettez à jour votre navigateur à une version récente.

2. Comment vérifier si un site web est sécurisé malgré l'erreur ?

Utilisez [Qualys SSL Labs](#) ou vérifiez le cadenas dans la barre d'adresse.

3. Quels risques y a-t-il à activer des versions anciennes de TLS ?

Elles sont considérées comme moins sécurisées et vulnérables à certaines attaques. Il est recommandé de ne les activer que temporairement et uniquement pour des sites de confiance.

4. Un VPN peut-il résoudre ce problème ?

Un VPN comme [NordVPN](#) garantit une connexion sécurisée et peut contourner certaines restrictions réseau qui perturbent les certificats SSL.

5. Dois-je contacter le support du site web si l'erreur persiste ?

Si l'analyse montre que le problème vient de leur certificat SSL ou de la configuration serveur, oui, contactez l'administrateur du site.

En suivant ce guide détaillé, vous aurez une solution adaptée à tous les cas possibles pour résoudre **ERR_SSL_UNSUPPORTED_VERSION** efficacement.