Résumé des points clés à retenir

Points clés	Explication
Qu'est-ce que l'erreur ERR_SSL_CERTIFICATE_TRANSPARENCY_REQUIRED ?	Une erreur liée à un certificat SSL non enregistré dans les journaux publics de transparence des certificats.
Impact principal	Empêche d'accéder au site Internet et compromet la sécurité.
Solutions côté propriétaire	Réémettre le certificat via la CA, mise à jour SSL, ajout aux journaux publics, mise à jour des navigateurs, etc.
Solutions côté utilisateur	Mettre à jour le navigateur, vider le cache/cookies, ou (temporairement) ignorer l'erreur.
Recommandations prioritaires	Travaillez avec une Autorité de Certification réputée (comme Let's Encrypt, GlobalSign) ou utilisez un VPN pour plus de sécurité.

---

1. Pourquoi cette erreur se produit-elle ?

Comprendre les origines de cette erreur est la première étape pour la résoudre efficacement.

- **Cause principale** : Le certificat SSL/TLS utilisé par le site web n'a pas été enregistré dans les *journaux publics de transparence des certificats (Certificate Transparency Logs)*. Ces journaux sont essentiels pour améliorer la sécurité globale de l'infrastructure HTTPS.
- **Contexte technique** : Depuis 2018, Google Chrome impose l'utilisation de ces journaux pour tout certificat TLS délivré après ce changement de politique.
- **Conséquence** : Les visiteurs des sites concernés voient l'erreur ERR_SSL_CERTIFICATE_TRANSPARENCY_REQUIRED lorsqu'ils tentent de naviguer sur ces pages.

---

2. Guide pas-à-pas pour les propriétaires de sites web

Les étapes suivantes vous aideront à résoudre de manière permanente l'erreur d'un point de vue propriétaire.

a) Contacter votre Autorité de Certification (CA)

1. **Vérifiez votre certificat** : Identifiez l'autorité qui a délivré le certificat (par exemple, Digicert, GlobalSign, Let's Encrypt, etc.).
2. **Expliquez le problème** : Indiquez que votre certificat n'est pas listé dans les *Certificate Transparency Logs*.
3. **Réémission du certificat** : La majorité des CA offriront une réémission gratuite de certificats pour résoudre de tels problèmes.
4. **Réinstaller le certificat** : Après réémission, installez de nouveau le fichier `.pem` ou `.crt` sur votre serveur.

b) Mettre à jour vos packages SSL/TLS

Assurez-vous que votre serveur est configuré de manière correcte, en mettant à jour les logiciels SSL/TLS utilisés :

- **Apache** : Vérifiez le fichier de configuration avec `ssl.conf` et redémarrez le serveur.
- **NGINX** : Modifiez le fichier de configuration, ajoutez le certificat mis à jour, et redémarrez avec `sudo systemctl restart nginx`.

c) Tester votre certificat

Utilisez des outils comme Qualys SSL Labs pour vérifier si votre nouveau certificat SSL est correctement configuré.

---

3. Guide pas-à-pas pour les utilisateurs finaux

Si vous êtes un utilisateur final et souhaitez accéder temporairement au site web, voici ce que vous pouvez faire.

Option 1 : Mettre à jour votre navigateur

1. Ouvrez Chrome, cliquez sur les trois points verticaux en haut à droite.
2. Sélectionnez **Aide > À propos de Google Chrome**.
3. Si une mise à jour est disponible, elle sera automatiquement appliquée.

Option 2 : Vider le cache et les cookies

1. Allez dans les **Paramètres > Confidentialité et sécurité**.
2. Cliquez sur **Effacer les données de navigation**.
3. Cochez "Cache" et "Cookies", puis cliquez sur **Effacer les données**.

Option 3 : Contourner l'erreur (non recommandé)

Vous pouvez temporairement charger le site via une invite Chrome :

1. Tapez `chrome://flags` dans la barre d'adresse.
2. Recherchez "**Certificate Transparency**".
3. Désactivez l'option temporairement, redémarrez votre navigateur.
4. ⚠ **Attention** : Cela réduit considérablement votre sécurité en ligne.

Option 4 : Activer un VPN sécurisé

Utilisez un service VPN comme NordVPN pour sécuriser vos connexions réseau. Cela permet souvent d'éviter les erreurs liées aux configurations SSL/TLS régionales.

---

4. Conseils d'expert

- **Travaillez avec des CA de confiance** : Les leaders comme GlobalSign ou Digicert incluent automatiquement les nouveaux certificats dans les journaux CT lors de leur émission.
- **Surveillez l'expiration du certificat** : Utilisez des solutions comme Wondershare Recoverit Data Recovery pour sauvegarder vos configurations SSL importantes.
- **Imposez HSTS** : Configurez HSTS (Strict Transport Security) sur votre serveur web pour forcer les connexions HTTPS sécurisées.

FAQ

1. Pourquoi mon certificat SSL n'est-il pas visible dans les *Certificate Transparency Logs* ?

Cela peut arriver si l'autorité de certification a omis de l’enregistrer ou si vous avez explicitement demandé son exclusion.

2. Puis-je résoudre ce problème sans contacter la CA ?

Non, la réémission ou une vérification auprès de la CA d'origine est essentielle.

3. Que faire si je rencontre cette erreur sur un site critique (banque, commerce en ligne) ?

Signalez le problème à l'administrateur du site et utilisez un VPN tel que NordVPN pour des connexions sécurisées dès que possible.

4. Ignorer l'erreur est-il sûr ?

Ce n'est pas recommandé. Vous risquez d’être exposé à des attaques man-in-the-middle ou d'autres menaces potentielles.

5. Combien coûte la réémission d'un certificat SSL ?

Cela dépend de l'autorité de certification, mais beaucoup offrent ce service gratuitement dans ce genre de cas.

Optimisez vos certificats SSL et évitez cette erreur grâce à une bonne gestion de vos outils. Que vous soyez développeur ou simple utilisateur, appliquez les étapes ci-dessus pour garantir une expérience web fluide et sécurisée.