Adaptation de la plateforme File Delivery Services (FDS)

Berne, juin 2024

Sécurité

Afin de protéger les données de nos clients et de la Poste, nous procéderons le **24 août 2024** aux adaptations techniques suivantes :

- La méthode d'échange de clefs «**diffie-hellman-group14-sha1**» sera désactivée.
- Le mode d'opération cryptographique « **aes128-ctr** » sera désactivé.
- Le MAC « **hmac-sha1** » sera désactivé.

Nous vous prions d'examiner vos logiciels de transfert des données et le cas échéant de les adapter. Si vos logiciels sont régulièrement mis à jour et prennent en charge les méthodes modernes de cryptage, ces adaptations n'auront aucune incidence sur votre utilisation de notre plateforme FDS.

Dans le cas où vous rencontreriez des problèmes lors de l'établissement de la connexion à notre serveur FDS après nos modifications, assurez-vous que votre logiciel de transfert prenne en charge les méthodes cryptographiques suivantes (il est essentiel qu'au moins une méthode par catégorie soit prise en charge) :

Algorithmes d'échange de clefs	Algorithmes de cryptage	MAC
curve25519-sha256	aes256-ctr	hmac-sha2-256
curve25519-sha256@libssh.org	aes256-gcm@openssh.com	hmac-sha2-512
diffie-hellman-group18-sha512	aes192-ctr	
diffie-hellman-group17-sha512		
diffie-hellman-group16-sha512		
diffie-hellman-group15-sha512		
diffie-hellman-group-exchange-sha256		

Informations et questions

questions techniques
Betrieb FDS
fds@post.ch

sécurité
I InfoSec
infosec@post.ch

La Poste CH SA
Informatique
Webergutstrasse 12
3030 Berne (Zollikofen)

E-Mail fds@post.ch