Anpassung File Delivery Services-Plattform (FDS)

Bern, Juni 2024

Sicherheit

Zum Schutz der Kunden- und Postdaten werden am **24. August 2024** folgende technische Anpassungen an der FDS-Plattform vorgenommen:

- Schlüsselaustauschverfahren mittels «**diffie-hellman-group14-sha1**» wird deaktiviert.
- das Verschlüsselungsalgorithmus «**aes128-ctr**» wird deaktiviert.
- der HMAC «**hmac-sha1**» wird deaktiviert.

Wir bitten Sie, Ihre Filetransfer-Software zu überprüfen und allenfalls entsprechend anzupassen. Sofern Ihre Software moderne Cipher Suites unterstützt, werden unsere Anpassungen keine Auswirkungen auf Ihre Nutzung der FDS-Plattform haben.

Falls Problem beim Verbindungsaufbau zur FDS-Plattform nach unseren Anpassungen auftreten, prüfen Sie, ob Ihre Filetransfer-Software die folgenden Kryptographischen Verfahren unterstützt (es ist notwendig, mindestens 1 Verfahren pro Kategorie zu unterstützen):

Key Exchange Methoden	Verschlüsselungsalgorithmen	MAC-Sicherung
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		

Informationen und Fragen

Technische Fragen
Betrieb FDS
fds@post.ch

Sicherheit
I InfoSec
infosec@post.ch

Post CH AG
Informatik
Webergutstrasse 12
3030 Bern (Zollikofen)

E-Mail fds@post.ch