Attualizzazione File Delivery Services-Plattform (FDS)

Berna, giugno 2024

Sicurezza

Per proteggere i dati dei clienti e della posta il **24 agosto 2024** verranno effettuate le seguenti modifiche tecniche alla piattaforma FDS:

- La procedura di scambio delle chiavi tramite « **diffie-hellman-group14-sha1**» verrà disattivata.
- L'algoritmo di crittografia "**aes128-ctr**" verrà disattivato.
- Il MAC "**hmac-sha1**" verrà disattivata.

Vi chiediamo di controllare il vostro software di filetransfer e, se necessario, di modificarlo. Se il vostro software e compatibile con le Cipher Suites moderne, le nostre modifiche non avranno nessun effetto sull'utilizzazione della piattaforma FDS.

Se si verificassero dei problemi quando si stabilisce una connessione alla piattaforma FDS, verificate se il software di filetransfer e compatibile con i seguenti processi crittografici (è necessario sostenere almeno 1 procedura per categoria):

Metodo Key Exchange	Algoritmi di crittografia	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		

Informazioni e domande

Domande tecniche
Betrieb FDS
fds@post.ch

Sicurezza
I InfoSec
infosec@post.ch

La Posta CH SA
Posta Informatica
Webergutstrasse 12
3030 Berna (Zollikofen)

E-Mail fds@post.ch