FWB FRANKFURTER WERTPAPIERBÖRSE

Xetra-Rundschreiben 131/18

Sicherheits-Upgrade für die Common Report Engine (CRE)

⚠ Aktion erforderlich

Zusammenfassung

Um eine zuverlässige und sichere Kommunikation mit der Infrastruktur der Common Report Engine (CRE) zu gewährleisten, wurden die SSH Key Exchange Algorithms, Ciphers und MACs aktualisiert.

Die in diesem Rundschreiben genannten Key Exchange Algorithms, Ciphers und MACs werden unterstützt. Diese Versionen können bereits jetzt genutzt und getestet werden, um eine Verbindung zur CRE herzustellen.

Bitte beachten Sie, dass veraltete – d. h. in diesem Rundschreiben nicht genannte – Key Exchange Algorithms, Ciphers und MACs, zum **10. März 2019** abgeschafft werden.

Vor diesem Hintergrund empfehlen wir unseren Handelsteilnehmern, ihre IT-Systeme zu prüfen und bis zum **10. März 2019** entsprechend anzupassen. Dies ist erforderlich, um einen störungsfreien Übergang zu gewährleisten, wenn die alten Versionen abgeschafft werden.

Datum: 17. Dezember 2018

Empfänger: Alle Xetra®-Teilnehmer und Vendoren

Autorisiert von:
i.A. Holger Patt,
i.A. Bernd Eschenbrücher

Zielgruppen:
- Technik
- Sicherheitsadministratoren
- Systemadministratoren
- Allgemein

Kontakt:
Ihr Technical Key Account Manager über Ihre VIP-Nummer oder per E-Mail an: cts@deutsche-boerse.com

Frankfurter Wertpapierbörse
Börsenplatz 4
60313 Frankfurt am Main
Postanschrift
60485 Frankfurt/Main

Internet:
www.xetra.com

Geschäftsführung
Hauke Stars (Vorsitzende),
Dr. Martin Reck (stv. Vorsitzender),
Dr. Cord Gebhardt, Michael Krogmann

Sicherheits-Upgrade für die Common Report Engine (CRE)

Um eine zuverlässige und sichere Kommunikation mit der Infrastruktur der Common Report Engine (CRE) zu gewährleisten, wurden die SSH Key Exchange Algorithms, Ciphers und MACs aktualisiert.

Die im Folgenden genannten Key Exchange Algorithms, Ciphers und MACs werden unterstützt. Diese Versionen können bereits jetzt genutzt und getestet werden, um eine Verbindung zur CRE herzustellen.

Bitte beachten Sie, dass veraltete – d. h. hier nicht genannte – Key Exchange Algorithms, Ciphers und MACs, zum 10. März 2019 abgeschafft werden.

Vor diesem Hintergrund empfehlen wir unseren Handelsteilnehmern, ihre IT-Systeme zu prüfen und bis zum 10. März 2019 entsprechend anzupassen. Dies ist erforderlich, um einen störungsfreien Übergang zu gewährleisten, wenn die alten Versionen abgeschafft werden.

Nur die folgenden Key Exchange Algorithms, Ciphers und MACs werden von der CRE unterstützt:

Key Exchange Algorithms:

- curve25519-sha256
- curve25519-sha256@libssh.org
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group-exchange-sha256
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

Ciphers:

- chacha20-poly1305@openssh.com
- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr

MACs:

- hmac-sha2-512-etm@openssh.com
- hmac-sha2-256-etm@openssh.com
- umac-128-etm@openssh.com
- hmac-sha2-512
- hmac-sha2-256

Die Beschreibung des Zugangs zur CRE ist im „Common Report Engine User Guide“ enthalten, der auf der Xetra-Website www.xetra.com unter dem folgenden Pfad abrufbar ist:

Technologie > T7-Handelsarchitektur > Systemdokumentation > Release 7.0 > Reports

Wenn Sie Fragen haben oder weitere Informationen benötigen, kontaktieren Sie Ihren Technical Key Account Manager über Ihre VIP-Nummer oder senden Sie eine E-Mail an: cts@deutsche-boerse.com.

17. Dezember 2018