NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to Empanelled Vendors/Application Service Providers(ASPs)

Circular No. : NCDEX/Member Tech Compliance-004/24

Date : July 12, 2024

Subject : Enhancement of API Authentication & Security for Exchange Empanelled Vendors (EV) and Application Service Providers (ASPs)

Securities Market participants and entities have been experiencing cyber-attacks/incidents which are rapidly growing in frequency and complexity. In view of the recent cyber-attacks/incidents reported to Exchanges, it is observed that several instances of Cyber-attacks were due to exploitation of vulnerabilities found in Application Programming Interface (APIs) which is used for critical products/applications at members' end. These vulnerabilities could result in sensitive data leakage or may cause business disruption due to unauthorized access of these APIs by threat actors.

Considering the seriousness of these security incidents attributed to vulnerable APIs used as a part of the software products/applications, the Exchange empanelled software vendors and ASPs are required to follow the below mentioned best practices.

Maintain Inventory of API: Inventory of API including ownership, criticality/impact of API shall be maintained.

Strong Authentication Mechanisms: Employ strong & mutual authentication mechanisms such as API keys, OAuth, or IWT, ensuring secure token management practices and setting appropriate expiration times.

Centralized API Security: Establish an API gateway for centralized security enforcement and a web application firewall (WAF) to protect against common web threats. Implement an API security gateway for both internal and external APIs. Disable any public API lacking secure authentication or strengthen it as per best practices at the earliest.

Data Protection and Secure Communication: Prioritize data protection by encrypting sensitive data, applying data masking techniques and using secure communication protocols to prevent eavesdropping and information leakage. Additionally, integrity checks through checksum or digital signature should be implemented to ensure data integrity & to avoid data manipulation/MITM.

Input Validation and Output Encoding: Validate and sanitize user inputs to prevent injection attacks and encode output to protect against HTML/JavaScript injection.

Rate Limiting and Throttling: Implement rate limiting and throttling mechanisms to prevent abuse and DDoS attacks, limiting requests from a single client within a specific time frame.

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com

Error Handling and Logging: Ensure proper error handling and comprehensive logging for monitoring and auditing purposes.

Cross-Origin Resource Sharing (CORS): Configure CORS properly to restrict unauthorized cross-origin requests.

Secure Storage of Secrets: Do not Store or Transmit API keys, credentials and sensitive data without secure encryption and access controls.

Regular Security Assessments: Conduct regular security assessments, including penetration testing, security audits, and code reviews. All APIs need to be assessed for security weakness/vulnerabilities and the checks should be aligned to OWASP Top 10 API security framework.

Documentation: Maintain clear documentation on secure API usage, including examples of proper authentication and authorization methods. For APIs facilitating sensitive business flows access shall be restricted on need-to-know basis.

Privacy Protection: Minimize data collection to essential information, comply with relevant privacy regulations and obtain user consent for data processing. Integrate privacy considerations from the initial stages of API development, performing a Privacy Impact Assessment (PIA) to identify and mitigate potential privacy risks.

Secure Software Development Lifecycle (SDLC): Integrate security considerations into the entire API development process and conduct security training for developers to promote secure coding practices.

Annual Software Audit (ISO 12207:2017): Conduct an annual software assessment as per ISO 12207:2017 standards for Systems and Software Engineering.

All Exchange Empanelled vendors/ASPs are required to comply with the above best practices.

For and on behalf of
National Commodity & Derivatives Exchange Limited

Ravindra Shetty
Senior Vice President – Member Tech Compliance

Registered Office: 1st Floor, Akruti Corporate Park, Near G.E. Garden, LBS Road, Kanjurmarg West, Mumbai 400 078, India. CIN No. U51909MH2003PLC140116
Phone: +91-22-6640 6789, Fax +91-22-6640 6899, Website: www.ncdex.com