
NATIONAL COMMODITY & DERIVATIVES EXCHANGE LIMITED

Circular to All Trading Members

Circular No. : NCDEX/Member Tech Compliance-005/24

Date : July 12, 2024

Subject : Advisory for Enhancement of API Authentication & Security for Trading Members

This is with reference to SEBI circular No.: SEBI/HO/MIRSD/CIR/PB/2018/147 dated December 3, 2018, and subsequent circulars regarding Cyber Security & Cyber Resilience framework for Stockbrokers. Securities Market organizations have been experiencing cyber-attacks which are rapidly growing in frequency and complexity.

Additionally, on analysis of these cyber-attacks reported by members in the past, it has been observed that these issues occurred due to vulnerable APIs used as part of the software products/services. To avoid occurrence of such cyber incidents and ensure secure usage of API, members are advised to adopt the following 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 advisory 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.

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 API's 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 Members are advised to take note of the above advisory

For and on behalf of
National Commodity & Derivatives Exchange Limited

Ravindra Shetty
Senior Vice President – Member Tech Compliance