भारतीय प्रतिभूति और विनिमय बोर्ड
Securities and Exchange Board of India

परिपत्र / CIRCULAR

HO/13/19/12(1)2026-ITD-1_CIMGI/10873/2026 ***05.05.2026***

प्रति,	**To,**
सभी ऑल्टरनेटिव इनवेस्टमेंट फंड (एआईफ)	**All Alternative Investment Funds (AIFs)**
सभी बैंकर टू इश्यू और सेल्फ-सर्टिफाइड सिंडीकेट बैंक (एससीएसबी)	**All Bankers to an Issue (BTI) and Self-Certified Syndicate Banks (SCSBs)**
सभी क्लीयरिंग कारपोरेशन	**All Clearing Corporations**
सभी कलेक्टिव इनवेस्टमेंट स्कीमें (सीआईएस)	**All Collective Investment Schemes (CIS)**
सभी क्रेडिट रेटिंग एजेंसियाँ (सीआरए)	**All Credit Rating Agencies (CRAs)**
सभी कस्टोडियन	**All Custodians**
सभी डिबेंचर ट्रस्टी (डीटी)	**All Debenture Trustees (DTs)**
सभी डिपॉज़िटरी	**All Depositories**
सभी डेसिग्नेटेड डिपॉज़िटरी पार्टिसिपेंट (डीडीपी)	**All Designated Depository Participants (DDPs)**
सभी डिपॉज़िटरी पार्टिसिपेंट (डिपॉज़िटरीज़ के जरिए)	**All Depository Participants through Depositories**
सभी निवेश सलाहकार (आईए) / अनुसंधान विश्लेषक (आरए)	**All Investment Advisors (IAs) / Research Analysts (RAs)**
सभी केवाईसी रजिस्ट्रेशन एजेंसियाँ (केआरए)	**All KYC Registration Agencies (KRAs)**
सभी मर्चेंट बैंकर (एमबी)	**All Merchant Bankers (MBs)**
सभी म्यूचुअल फंड (एमएफ) / असेट मैनेजमेंट कंपनियाँ (एएमसी)	**All Mutual Funds (MFs)/ Asset Management Companies (AMCs)**
सभी पोर्टफोलियो प्रबंधक	**All Portfolio Managers**
सभी रजिस्ट्रार टू इश्यू और शेयर ट्रांसफर एजेंट (आरटीए)	**All Registrar to an Issue and Share Transfer Agents (RTAs)**
सभी स्टॉक ब्रोकर (एक्सचेंजों के जरिए)	**All Stock Brokers through Exchanges**
सभी स्टॉक एक्सचेंज	**All Stock Exchanges**
सभी वेंचर कैपिटल फंड (वीसीएफ)	**All Venture Capital Funds (VCFs)**

महोदय/महोदया,

Dear Sir/Madam,

विषय: खामियों (वल्नरेबिलिटी) का पता लगाने के लिए आए नए-नए एडवांस्ड एआई टूल (जैसे Mythos) के संबंध में एडवाइज़री

Subject: Advisory on Emerging Advanced Artificial Intelligence (AI) Tools for Vulnerability Detection (like Mythos)

क. खामियों (वल्नरेबिलिटी) का पता लगाने वाले नए-नए एआई टूल (जैसे Claude Mythos) आने लगे हैं, जिनकी बदौलत विनियमित (रेग्यूलेटेड) एंटिटियों के सामने नए-नए जोखिमों की आशंकाएँ पैदा हो रही हैं । जैसा कि ये टूल बड़ी तेजी से और बड़े पैमाने पर काम करते हैं, तो यह मुमकिन है कि इनकी बदौलत जोखिमों की आशंका भी काफी बढ़ जाए । इसके अलावा, यह भी मुमकिन है कि डाटा की गोपनीयता भी खतरे में आ जाए, ऐप्लिकेशन की विश्वसनीयता पर भी सवाल खड़ा हो, और तो और उसके नतीजों को लेकर भी भरोसा न हो ।

A. The rapid evolution of emerging technologies including AI-driven vulnerability identification tools (E.g. Claude Mythos) has introduced new dimensions of risks for Regulated Entities. Such tools may give rise to heightened risk exposure by enabling identification and potential exploitation of existing vulnerabilities using speed and scale. It may also introduce concerns relating to data confidentiality, application integrity and reliability of outputs.

ख. जैसा कि सिक्यूरिटीज़ मार्केट की समूची व्यवस्था में सभी मार्केट पार्टिसिपेंट्स का एक-दूसरे से सरोकार भी रहता है और उनकी एक-दूसरे पर निर्भरता भी रहती है, इसीलिए यह जरूरी है कि इनकी खामियों (वल्नरेबिलिटी) को दूर करने, जानकारी एक-दूसरे से साझा करने और इन पर नज़र रखने / इनका आकलन करने के लिए एक साझा प्रयास किया जाए, ताकि कहीं ऐसा न हो कि किसी एक जगह या किसी एक पर अगर आँच आए तो उसका असर ताश के पत्तों की तरह दूसरी जगह या दूसरों पर भी बिखरता नज़र आए ।

B. Due to the interconnectedness and interdependency of market participants in the Securities Market Ecosystem, a periodic coordinated approach for vulnerability management, information sharing and monitoring/assessment is required to prevent a cascading impact.

ग. उपरोक्त के मद्देनज़र, एक कार्य-दल (टास्क फोर्स), जिसका नाम **cyber-suraksha.ai** है (ईमेल आईडी: project-cyber-suraksha.ai@sebi.gov.in) बनाया गया है, जिसमें MIIs, QRTAs, सभी QREs और दूसरे संबंधित स्टेकहोल्डर्स के प्रतिनिधियों को शामिल किया गया है । इस कार्य-दल के मुख्य कार्य इस प्रकार हैं:

i. बारीकी से यह जाँचना कि एआई वाले मॉडल से साइबर सुरक्षा को लेकर क्या-क्या जोखिम हो सकते हैं और ऐसे मॉडल की वजह से पैदा हो सकने वाले जोखिमों से निपटने के लिए एकसमान नीति निधारित करना ।

ii. अगर किसी खतरे की आशंका की कोई जानकारी मिले, तो उसे साझा करना; खामियों (वल्नरेबिलिटी) को दूर करने के लिए अपनाए जाने वाले बेहतरीन तरीकों की जानकारी साझा करना; यह जानकारी साझा करना कि खतरों से कैसे निपटा जाए।

iii. सिक्यूरिटीज़ मार्केट में साइबर सुरक्षा की व्यवस्था को और पुख्ता करने के लिहाज से साइबर हमलों की, गड़बड़ी की हो रही कोशिशों की या बड़े हमलों की तत्काल सूचना देना, खामियों (वल्नरेबिलिटी) आदि की तत्काल सूचना देना ।

iv. यह समीक्षा करना कि थर्ड पार्टी ऐप्लीकेशन सर्विस प्रोवाइडर्स (सूची में शामिल वेंडरों सहित) के यहाँ साइबर सुरक्षा की व्यवस्था कैसी है ।

C. In view of the above, a task force, namely **cyber-suraksha.ai**, (email id: project-cyber-suraksha.ai@sebi.gov.in) has been constituted comprising representatives from MIIs, QRTAs, all QREs, and other related stakeholders with the following mandate to:

i. Closely examine the cybersecurity risks posed by AI based models and devise a uniform mitigation strategy against the risks posed by such models.

ii. Facilitate sharing of threat intelligence, best practices on vulnerability management, use cases and playbooks to respond to the threat vector etc.

iii. Report on a priority basis, cyber incidents or malicious activities, significant attack vectors, information on vulnerabilities etc. that may be relevant to strengthen the cyber security posture of the securities markets.

iv. Review the cyber security posture of the third party application service providers including empaneled vendors.

घ. Mythos जैसे एआई प्लेटफॉर्म की वजह से पैदा हो सकने वाले जोखिमों की समीक्षा करने और उनसे निपटने के लिए उठाए जाने वाले कदमों के बारे में चर्चा करने के लिए MIIs और QRTAs के साथ कार्य-दल (टास्क फोर्स) cyber-suraksha.ai की एक बैठक बुलाई गई थी । कार्य-दल (टास्क फोर्स) की इस बैठक में हुए विचार-विमर्श के आधार पर, एक एडवाइज़री **संलग्नक-क (Annexure-A)** के रूप में संलग्न है ।

D. A meeting of the task force **cyber-suraksha.ai** was convened (with MIIs and QRTAs) to review the risks posed by AI platforms like Mythos and discuss the mitigation measures. Based on the consultation with the said task force, an advisory is enclosed at **Annexure-A**.

ङ. इस एडवाइज़री के साथ-साथ सेबी के लागू परिपत्रों (सर्कुलर्स) [जिनमें साइबर सुरक्षा और साइबर हमलों से निपटने की क्षमता के ढाँचे के संबंध में जारी किया गया परिपत्र शामिल है] और सेबी द्वारा बाद में समय-समय पर किए जाने वाले अपडेट पर भी अवश्य गौर किया जाए ।

E. This advisory should be read in conjunction with the applicable SEBI circulars (including but not limited to Cybersecurity and Cyber Resilience framework) and any subsequent updates issued by SEBI from time to time.

च. यह परिपत्र (सर्कुलर) भारतीय प्रतिभूति और विनिमय बोर्ड अधिनियम, 1992 (सेबी एक्ट, 1992) की धारा 11(1) [जो सिक्यूरिटीज़ मार्केट में निवेश करने वाले निवेशकों के हितों की रक्षा करने और सिक्यूरिटीज़ मार्केट के विकास को बढ़ावा देने और उसे विनियमित (रेग्यूलेट) करने से संबंधित है] के तहत प्रदान की गई शक्तियों का प्रयोग करते हुए जारी किया जा रहा है ।

F. This circular is issued in exercise of powers conferred under Section 11 (1) of the Securities and Exchange Board of India Act, 1992, to protect the interests of investors in securities and to promote the development of, and to regulate the securities market.

भवदीया Yours Faithfully,

ममता रॉय Mamata Roy
उप महाप्रबंधक
Deputy General Manager
दूरभाष / Phone: 022-26449599
ईमेल / Email: mamtar@sebi.gov.in

Annexure-A

1. Update all operating systems and applications with the latest patches on immediate basis to mitigate any identified/known vulnerabilities. As an interim measure for the vulnerabilities where patches are not available, virtual patching can be considered for protecting systems and networks.

2. Conduct Vulnerability Assessment (Using conventional and suitable AI based Vulnerability Assessment Tools where possible) and undertake security audits on a regular/continuous basis in accordance with Cyber Security and Cyber Resilience Framework of SEBI.

3. Engage with the respective RE's third party vendors to release timely patches and deploy them appropriately. Exchanges and Depositaries shall direct their empaneled application vendors (providing COTS solution to respective members) to undertake comprehensive assessment of the risks arising from the use of AI-led vulnerability detection models. Based on the assessment, vendors shall implement appropriate safeguards including updating patch, VAPT, continuous monitoring, hardening measures etc.

4. **Change Management:** Any change in the systems (including minor changes) should encompass full documentation, thorough impact analysis, structured review, rigorous testing and secure deployment to ensure operational resilience and system stability.

5. **API Security:**

    a) Inventory of all APIs and the applications using the APIs should be updated regularly.
    b) Ensure strong authentication and authorization mechanisms to enable secure verification of end-user client identity as well as limit the information access/ transfer to users/ systems based on least privilege.
    c) API rate limiting and throttling to prevent and detect abuse.
    d) Connections through APIs to be strictly on a whitelist-based approach.

6. **SOC Monitoring:**

a) Regular day-to-day monitoring of the systems and networks must be carried out vigorously. SOC alerts should be adequately examined including the low-priority alerts.
b) Implement enhanced security orchestration and Automated Response (SOAR) playbooks integrated with Security Incident and Event Management (SIEM) solutions, after thorough testing wherever feasible.
c) The Market SOC (M-SOC), established by NSE and BSE, which serves as a centralized security platform, provides 24x7 real-time monitoring and threat detection across digital infrastructure. In the view of enhanced risks posed by AI-driven attacks, all eligible REs (not on boarded with any M-SOC) shall expedite the onboarding.
d) MIIs are required to conduct awareness and handholding programs, including periodic workshops to ensure a smooth onboarding process and integration with M-SOC.

7. **Risk Assessment:** The Cyber Security and Cyber Resilience Framework (CSCRF) of SEBI has mandated periodic Risk Assessment of the REs including their Third Party Service Providers to enhance visibility and conduct a reasonably accurate assessment of the overall cybersecurity risk posture. Risk assessment shall include comprehensive scenario-based testing for assessing risks (including both internal and external risks) related to cybersecurity in REs' IT environment. The capability of AI based models may also be considered as one of the risk scenarios.

8. Implement system hardening by adopting secure configurations, disabling unnecessary services and default accounts, and enforcing solutions like least privilege, Zero Trust Network (ZTNA) to minimize the attack surface.

9. Periodically update Asset Inventory and Software Bill of Materials for all critical applications including open source stack.

10. MIIs and other Regulated Entities shall seek guidance from their respective IT committees for mitigating risks emanating from AI-led vulnerability detection models. Further, all REs need to prepare a long-term plan for usage of AI in detection and autonomous/agentic mitigation. Also, undertake other measures including recalibration of risks for AI accelerated threats, AI augmented SOC transformation, and continuous vulnerability management using AI tools.

****