

Circular No.: NSDL/POLICY/2023/0182

December 26, 2023

Subject: Compliance to SEBI Circulars, Guidelines and Advisories.

This is in reference to the recent advisory from SEBI regarding the possible security risks in some vendor products. This advisory pertains to critical vulnerabilities identified in certain vendor products, which, if left unaddressed, could jeopardize the security and integrity of your data and systems.

For your convenience, we have enclosed the 'Annexure' below detailing the affected vendors, products, and the specific vulnerabilities identified. We advise for your immediate attention to the following actions:

1. Review the enclosed document to determine if any of the listed products are in use within your operational environment.
2. Conduct a thorough assessment of your systems and applications to identify any issues associated with the aforementioned products. If any vulnerabilities are identified, please provide a timeline for their resolution.
3. Report any vulnerabilities that may have significant implications for the broader financial system.

Additionally, it is imperative that you confirm your adherence to the guidelines, rules, and regulations set forth by SEBI in relation to system/cyber audit, VAPT, cloud framework, incident reporting, and AI/ML reporting, among others.

Participants are advised to take note of the above and ensure immediate compliance.

**For and on behalf of
National Securities Depository Limited**

**RAKESH M
MEHTA**
Digitally signed by
RAKESH M MEHTA
Date: 2023.12.26
15:57:23 +05'30'

**Rakesh Mehta
Vice President**

FORTHCOMING COMPLIANCE			
Particulars	Deadline	Manner of sending	Reference
Investor Grievance Report (Monthly)	By 10 th of the following month	Through e-PASS	1. Para 20 of NSDL Master Circular for Participants on 'Grievance Redressal' chapter. 2. Circular No.: NSDL/POLICY/2023/0161 dated November 13, 2023

**National Securities Depository Limited**

4th Floor, 'A' Wing, Trade World, Kamala Mills Compound, Senapati Bapat Marg, Lower Parel, Mumbai – 400 013, Maharashtra, India
Tel.: 91-22-2499 4200 | Fax: 91-22-2497 6351 | email: info@nsdl.com | Web: www.nsdl.co.in
Corporate Identity Number: U74120MH2012PLC230380

Annexure

Sr No.	Vendor	Product	Vulnerabilities
1	Symphony Fintech Solutions Pvt. Ltd	Used for front-office (IBT) XTS Web Trading Platform & XTS Mobile Trading Platform	Weak Authorization leads to Account takeover, broken access control, and PII data leak
2	63moons	Used for front-office (IBT) Wave 2 and Aero	Weak Authorization leads to Account takeover, bypass 2FA, and PII data leak
3	Apex Softcell (India) Private Limited	LD Mobile Back-Office Software (LdMobileService) and LD Client Level Back Office (LDClientLevel)	Weak Authorization leads to PII data leak
4	Shilpi Computers Pvt. Ltd	Backoffice: Shilpisoft client-dashboard and Shilpisoft CapexWeb (NetbackOffice)	Weak Authorization leads to PII data leak. Shilpisoft client dashboard is hosted on webappreports.com for all clients
5	Meon Technologies Pvt. Ltd	Used for onboarding (ekyc), IPO, rekyc, etc	Weak authorization and file management leading to access to PII data. Some brokers host APIs on vendor servers which can lead to a single point of failure
6	TechExcel Software Solutions Pvt. Ltd	Backoffice	Weak Authorization leads to PII data leak
7	Reedos Software Solutions Pvt Ltd	Mutual fund product	Weak Authorization leads to PII data leak

