GOVERNMENT OF INDIA
MINISTRY OF FINANCE
DEPARTMENT OF ECONOMIC AFFAIRS

LOK SABHA

UNSTARRED QUESTION NO: 190

TO BE ANSWERED ON 29TH NOVEMBER, 2021/ AGRAHAYANA 8, 1943 (SAKA)

CDSL'S KYC API

190: SHRI MANISH TEWARI

Will the Minister of FINANCE be pleased to state:

(a) whether it has come to the notice of the Government from any source, public or private, that there is an authorization vulnerability in CDSL's KYC API, leading to exposure of massive amounts of sensitive data on the internet;

(b) if so, the assessment of the vulnerability that has come to the notice of the Government and whether it has taken measures to secure this vulnerability;

(c) if not, the steps that the Government is actively undertaking to detect such threats and vulnerabilities in the CDSL's KYC API; and

(d) whether there have been any other cases of similar data leaks or KYC frauds and if so, the details thereof?

ANSWER

SHRI PANKAJ CHAUDHRY

MINISTER OF STATE FOR FINANCE

(a): There has been no reported authorization vulnerability in any of the Application Programming Interfaces (APIs) and / or website of Central Depository Services Ltd. (CDSL). However, vulnerability in the website of CDSL Ventures Limited (CVL), which is a subsidiary of CDSL and registered as KYC Registration Agency (KRA) with SEBI, was reported.

(b) & (c): National Critical Information Infrastructure Protection Centre (NCIIPC) reported on October 20, 2021 that the web portal of CVL is vulnerable to Insecure Direct Object References. It was initially observed that on the login page of CVL, there was a possibility of getting access to the details of another user by changing the reference ID of the user. The

issue pertains to a specific page in CVL website and is not related to any APIs. The vulnerability was mitigated by CVL on October 26, 2021 with a quick fix by encrypting the reference ID, which was getting passed as a clear text. Second vulnerability alert was received by CVL on October 31, 2021. Since development was already underway at CVL for a permanent fix, the vulnerability was mitigated on the same day and confirmed to Indian Computer Emergency Response Team (CERT-In). A forensic audit was also conducted as directed by Securities and Exchange Board of India (SEBI). The external auditor of CVL also checked and certified that the reported vulnerability has been closed.

NCIIPC was set up by Government of India under Section 70A of the Information Technology Act, 2000 through a gazette notification on 16 Jan 2014 and is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection. It takes all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders. CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. SEBI has also laid down a detailed framework with regard to cyber security and cyber resilience for KRAs, vide SEBI circular dated October 15, 2019.

(d): SEBI has not reported any other cases of data leaks or KYC frauds in respect of KRA.

***