Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:132 **01-04-2021**

Name: Security controls improvement in Telecom Operators

Threat Classification: Security controls Evasion

Summary:

During an investigation of a CS incidence by LEA, an intrusion activity has been noticed with an attempt to bypass the security systems (controls) deployed by some Operators/ Licensee using the known vulnerabilities related to SolarWinds product, for which an advisory has already been issued. Keeping in view, following security recommendations are forwarded for strict compliance.

S. No.	Recommendations	Applicable to
1	All licensees should manage their servers within Pakistan, as per the license awarded to them, which clearly mentions to establish, maintain and operate in Pakistan.	All Licensees
2	Bind static IP address with user accounts for API / Web portal	All Licensees
3	Access to foreign IP address should be blocked through geo-fencing at firewalls (where international links are not involved)	All Licensees
4	Two factor authentication (2FA) be used for all customers for every login to SMS application	All Licensees
5	Maintain all types of logs including but not limited to Access Log, Events Log, "Failed Login Attempts with complete IP details" and "API failed connections", in accordance with clause 6 (5) of CTDISR 2000, issued by PTA	All Licensees

6	Dedicated / Managed services of Web Application Firewall (WAF) be used to secure networks from layer 7 attacks	All Licensees
7	Password baselining restrictions be implemented	All Licensees
8	Security from roaming SMS links be ensured	Whoever is providing service
9	Web links in the SMS content be blocked, as it generally refers to phishing links	SMS Aggregator / CMOs
10	Personal Data Requests should not be allowed in the SMS	SMS Aggregator / CMOs

Compliance Deadline:

- Deadline for the compliance submission is **30-04-2021**.