F. No. 1/6/2011-IT-IV (236746)
Government of India
Ministry of Power

Shram Shakti Bhawan, Rafi Marg,
New Delhi, Dated: 9th October, 2018

To

Additional Chief Secretary, Principal Secretary, Secretary (Energy) of States/UTs

Subject : Guidelines for Mitigation of Cyber Secuirty Threats in Power Sector .

Sir,

I am directed to convey that National Critical Information Infrastructure Protection Centre (NCIIPC) has found following vulnerabilities while conducting cyber security assessment at two Discoms in the country:

(i) Due to lack of patch/update management, the Operating Systems of servers are prone to multiple critical security vulnerabilities such as "Shell Shock", " Remote Code Execution" and are open to various kinds of attacks.

(ii) Applications installed over servers are not being patched to the latest patches/updates and are prone to multiple security critical vulnerabilities and susceptible to different kind of cyber attacks (eg. Oracle Database used in server is having unsupported patches level).

(iii) The team was able to access the Oracle Database remotely over Internet by Exploiting SQL Injection vulnerabilities.

(iv) Telnet services have been configured over services, which provides remote login for administration. As Telnet transmits traffic in clear text, attackers may sniff into the traffic and steal Telnet credentials.

(v) Server is configured with SNMP (Simple Network Management Protocol ) community string. An attacker could leverage knowledge of a SNMP community string to collect sensitive information such as device configuration, installed software, running processes, installed patches, network configuration, network connections etc.

(vi) Windows firewall was found disabled on the NMS (Network Management System) server.

(vii) Web and Directory Servers are having high web vulnerabilities such as SQL Injection, Cross Site Scripting. etc.

(viii) Servers have not been hardened, and contain unnecessary services, which increase attack surface sustainability.

(ix) VNC (Virtual Network Computing) Application, third party application, was running on Human Machine Interface (HMI) Workstations which allow remote logon to the systems, hence usage of VNC exposes large attack surface.

(x) Operating systems of Workstations do not have windows security polices such as Password Policy, Account Lockout etc.

(xi) No active Anti-Virus application was found on the workstation. This is a critical vulnerability and a serious threat.

(xii) The switch/Router was configured with the default credential. Default credential may allow attacker to compromise the entire network at ease.

(xiii) There is no end to end communication between RTUs and FEP Server. The communication between RTUs and LDMS is in plain text. This may allow attackers to inject commands, sniff and modify traffic.

(xiv) Definition database of Cyberoam Firewall was found to be un-updated, which leave the entire network prone to various kinds of cyber attacks.

(xv) Many of the Passwords were weak and the team could easily crack the hashes to retrieve the password in plain text.

2. National Critical Information Infrastructure Protection Centre (NCIIPC) has issued following guidelines regarding Cyber Security threats in Power Sector and are conveyed for further necessary action and compliance:

(i) Deploy only those critical software application such as Anti-Virus applications, whose technical support and version control are verifiable publically.

(ii) Deploy product releases and firmware update and technical support details which are not available in the open domain.

(iii) Evolve procedural controls such as Security Level SLA which mandates the OEM/System-Integrator & makes him liable to provide/support security patches and firmware updates for longer duration on equipment life cycle.

(iv) Avoid Internet connectivity directly or indirectly (over firewall) to OT/SCADA networks.

(v) Update all Operating Systems, Applications and Firmware as a basic cyber hygiene practice.

(vi) Nominate CISO (Chief Information Security Officer), ISOs' (Information Security Officer) to establish ISD (Information Security Department) for implementing and managing information security at different location of the organisation.

(vii) Accelerate the process of CII identification and notification as Protected Systems, steered by Power Sector CERTs.

Yours faithfully,

(Praveen Kumar)
Under Secretary to Government of India
Telefax; 23715507 extn. 370
it-mop@nic.in

Copy to:

1. MDs of All DISCOMs
2. CISO-MoP for Necessary compliance