Subject: - **Cyber Security Advisory - APT Hackers Targeting Industrial Control Systems with ShadowPad Backdoor (Advisory No. 29)**

Context. Reportedly, a threat actor of APT group is targeting ICT infrastructure of Pakistan by exploiting **Microsoft Exchange proxy logon** vulnerabilities and Server-Side Request Forgery (**SSRF**) vulnerabilities (CVE-2021-26855).

2. **Vulnerability Details**

a. The above mentioned vulnerability exists in Microsoft Exchange Server that allows an attacker to impersonate as **Admin** and **Execute arbitrary file** to get **Remote Code Execution** (**RCE**) access. By exploiting this vulnerability, attackers can execute **arbitrary commands** on remote Microsoft Exchange Server.

b. This vulnerability affects **Exchange 2013 versions below 15.00.1497.012, Exchange 2016 CU18 below 15.01.2106.013, Exchange 2016 CU19 below 15.01.2176.009, Exchange 2019 CU7 below 15.02.0721.013** and **Exchange 2019 CU8 below 15.02.0792.010**. All components are vulnerable by default.

c. After exploiting respective vulnerability, attackers can drop **anti-forensic** and **anti-analysis** techniques through a malware to **bypass local defenses** and get access to data rich servers / Industrial Control Systems (ICS) and confidential information.

3. **Recommendations**. In this regard, few recommendations (**but not limited to**) to protect ICS are as follows: -

a. Update and upgrade Microsoft Exchange Server to **latest version**.

b. Use effective perimeter controls to isolate **ICS/SCADA systems** and networks from internet and **restrict communications entering or departing ICS/SCADA perimeters**.

c. Impose **Multifactor Authentication** for all remote access to ICS networks and devices.

d. Create a plan for **handling cyber incidents**.

e. Regularly **change all passwords for ICS/SCADA devices** and **systems**. Never use default passwords to prevent brute-force attacks.

f. Keep **offline backups** and check integrity and hash of firmware and controller configuration files to ensure that the backups are legitimate.

g. **Restrict network connections** that are specifically authorized for use with ICS/SCADA systems.

h. Install EDR and configure Device Guard, Credential Guard and Hypervisor Code Integrity to stably secure management systems (**HVCI**).

i. Implement reliable management network and ICS/SCADA system log collection and retention.