Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:11X **10-08-2021**

Name: Early Warning & High Alert – Prevention against Hacking attempts on National Days (14th Aug, 6th Sep, 2021)

Threat Classification: Hacking, Defacement, Denial of Service (DoS)

Context:

All Telecom licensees are notified through an early warning to take the necessary steps to prevent and minimize the impact of cyber-attacks, espionage, and sabotage. Various hostile elements, launch offensive operations to cripple critical services and infrastructure of Pakistan. 2017-2020 Trend analysis shows high frequency of reported hacking and defacement activity on official websites including government and ministries allegedly by Indian hackers.

Implications of Cyber-Attacks on National Day:

Hackers perform malicious activities on National Days i.e. Independence Day, Defense day and similar national events, having serious consequences. Details are as under: -

a) **Display of anti-state content on national websites (Website hacking, defacement)**

b) **Unavailability of online services (Denial of Service attack).**

c) **Breach and loss of critical or sensitive national data (Exfiltration)**

Hackers Strategy:

Hackers are using multiple **techniques** to **deface websites** and gain **illegitimate** access not limited to following technical means:

a) **SQL injection attack**

b) **Buffer Overflows attack**

c) **Cross Site scripting (XSS) attack**

d) **Input validation attack**

e) **Cross request forgery (CSRF) attack**

f) **XML external entity XXE attack**

g) **Denial of Service (DoS) attack**

h) **URL based attacks**

i) **And other latest and evolved techniques**

Remedial Measures:

- **For Immediate Actions**
  - Input sanitization on public-facing/internet exposed websites and services.
  - Implement secure login sessions.
  - Do not save configuration files in public folders. Store in encrypted format.
  - Disable unnecessary services, ports, protocols, modules and anonymous accounts.
  - Disable remote access of Database Servers.
  - Enable fraud warning features where available.
  - Whitelist IP addresses where admin panel is accessible.
  - Disable server-info and signatures.
  - Do not run webservers as 'root'.
  - Inspect passphrases for use of any weak or default log-in credentials.
  - Assign minimal privileges on administrator accounts, multifactor authentication and defined authorization procedures.
  - Install, enable, and update Web Application Firewall (WAF) and Anti-DDoS protection; ensure control properly functioning for on-time and automated detection and prevention.
  - Inspect the contents and latest back-ups of the public-facing/internet exposed site and services for hidden malware and vulnerabilities. Remove all critical vulnerabilities.
  - Ensure 24/7 security monitoring of critical infrastructure, services and websites for proactive remediation and response to any detected/observed abnormal activity.
  - Update CMS, webservers with latest plugins, releases, security patches.
  - Identify point of contact (and a back-up) for incident response.
  - Contact the vendor/third party/service provider, to ensure appropriate security measures and report any abnormal activities if you have hosted website on their platforms.

For Best Practices

- Follow secure code development and maintenance practices for public exposed websites and services.
- Properly harden all public exposed websites and services.
- Properly harden all Firewalls, routers, switches and network nodes.
- Properly harden DNS and Email services.
- Train employees on social engineering and incident response procedures.
- Update Plug-ins to fix bugs, patch security issues, install updates on web servers.
- Schedule regular back-ups of database.

In case of an Incident

- Replace the website with a maintenance page immediately
- Inform relevant parties of the incident (e.g. regulator, management, customers etc.)
- Make a statement to the public to preserve your organization's reputation.
- Restore your website with back-ups to ensure quick recovery.
- Report the incident to law enforcement authorities.
- Have technical support and RCA (root cause analysis) of the incident to analyze how the website was defaced and evaluate the process of response (e.g. to improve for any future complications).

Recommendations

- Strictly follow all mitigation measures mentioned above.
- Perform vulnerability assessment and penetration testing of websites and exposed services and remediate the identified vulnerabilities and weaknesses at earliest.
- Employ trained and dedicated resources for critical services and data protection.