F. No. 3(5)/2023-NTISB-EW
Government of Pakistan
Ministry of Science & Technology
******

Islamabad, the 12th September, 2023

Rector, COMSATS Islamabad	Chairman, PSF, Islamabad	Chairman, PCSIR, Islamabad	Chairman, PCST, Islamabad
Rector, NUST, Islamabad	Director General, NIO, Karachi	Director General, PSQCA, Karachi.	Chairman, PEC, Islamabad
Rector, NUTECH, Islamabad	Chairman, CWHR, Karachi	Director General, PNAC, Islamabad	Managing Director, STEDEC, Lahore.
Director General, PCRET, Islamabad	Director General, NIE, Islamabad	Managing Director, NEECA, Islamabad	Director General, PHA, Islamabad

Subject:

Cyber Security Advisory – Power Management Software Vulnerability in Data Centers (Advisory No. 51)

Cyber Security Advisory – WinRAR Critical Vulnerability Exploitation via Phishing Emails (Advisory No. 52)

Cyber Security Advisory – Prevention Against Financial Scam Activities – Impersonation as Govt Officials (Advisory No. 53)

Cyber Security Advisory – Secure Email Communications (Advisory No. 54)

Dear Sir / Madam,

Please find enclose herewith the subject advisories received from National Telecom and Information Technology Security Board (NTISB) Cabinet Division, for information and strict compliance.

Encl: **As above.**

(Engr. Asif Akhtar Mughal)
Deputy Electronics Adviser-II
051-9206041

Copy for information to:

I. Network Administrator, MoST

II. APS to JEA, MoST

-97-

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)
*****

12/9

No. 1-5/2003 (NTISB-II)

Islamabad, the 1st September, 2023

Subject: **Cyber Security Advisory - Power Management Software Vulnerability in Data Centers (Advisory No. 51)**

Recently, **Trellix**[1] Advance Research Center has uncovered a number of vulnerabilities in **CyberPower's**[2] PowerPanel Enterprise, Data Center Infrastructure Management **(DCIM)**[3] platform and **Dataprobe's**[4] iBoot Power Distribution Unit (PDU). Details are given in ensuing paras:

2. Summary of Vulnerabilities

a. Following 4 x major vulnerabilities in CyberPower's PowerPanel Enterprise and 5 x critical vulnerabilities in the Dataprobe's iBoot PDU have been reported:

(1) **CyberPower's PowerPanel Enterprise**. CyberPower's PowerPanel Enterprise DCIM platform allows IT staff to manage, configure and monitor the infrastructure within a data center serving as a single source of information and control for all devices. The reported vulnerabilities are as follows:

(a) **CVE-2023-3264:** Use of hard-coded credentials (CVSS 6.7)

(b) **CVE-2023-3265:** Improper neutralization of escape, Meta or control sequences (Auth Bypass; CVSS 7.2)

(c) **CVE-2023-3266:** Improperly implemented security check for standard (Auth Bypass; CVSS 7.5)

(d) **CVE-2023-3267:** OS command injection (Authenticated RCE; CVSS 7.5)

(2) **Dataprobe iBoot PDU**

(a) **CVE-2023-3259:** Deserialization of untrusted data (Auth Bypass; CVSS 9.8)

(b) **CVE-2023-3260:** OS command injection (Authenticated RCE; CVSS 7.2)

(c) **CVE-2023-3261:** Buffer overflow (DOS; CVSS 7.5)

[1] **Trellix** is a cyber security company, based in USA.
[2] **CyberPower** is a USA based company to design and manufacture a wide range of innovative power products, PDUs and Power management systems.
[3] **DCIM** tools monitors, measure, manage datacenter utilization and energy consumption.
[4] **Dataprobe** is an American manufacturer of system for minimizing downtime to critical data.

DEA-III/ 12/09/2023

SECRETARY MO
Dy. No. 3358
Dated 12-9-23

Additional Secretary MoST
Dy.No. 2585
Date 12/9/23

AS	
JS (Admin)	
JS (Org)	
CFAO	
JEA	✓
JTA	
JSA (IL)	
JSA (P&C)	
AO (Legal)	

12/9

DEA-II
Dy. No 50
Date: 12.9.2023

JEA
Dy. No. 902
Dated 12-9-2023

AS DEA-II

DEA-III

12/9/23

Plz circulate 12-9-23

12/9/2023

98

(d) **CVE-2023-3262:** Use of hard-coded credentials (CVSS 6.7)

(e) **CVE-2023-3263:** Authentication bypass by alternate name (Auth Bypass; CVSS 7.5)

b. **Impact**. Following implications are foreseen after exploitation of the above-mentioned vulnerabilities by an attacker:

(1) By accessing power management system, attacker can control devices connected to a PDU and manipulate power management to damage the hardware devices.

(2) Unauthorized access to data center systems, thus allowing the attacker to switch off the power and infect data center to utilize compromised resources and further initiate attacks at large scale.

(3) Both products are vulnerable to remote code injection, thereby, attacker can install a backdoor and exploit system and devices.

3. **Recommendations**

a. PowerPanel Enterprise and Dataprobe iBoot PDU are recommended to be updated to the following versions:

(1) PowerPanel Enterprise software - **Version 2.6.9.**

(2) Dataprobe iBoot PDU firmware - **Version 1.44.08042023.**

b. Ensure PowerPanel Enterprise or iBoot PDU should be reachable only from organization's secure intranet.

c. In case of the iBoot PDU, disable remote access via Dataprobe's cloud service as an added precaution.

4. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

59

No. 1-5/2003 (NTISB-II)

Islamabad, the 8 September, 2023

Subject: - **Cyber Security Advisory – WinRAR Critical Vulnerability Exploitation via Phishing Emails (Advisory No. 52)**

Reportedly, hackers are targeting users with improvised phishing email containing attachments of password protected WinRAR zip files. Upon unzipping the rare files, malware automatically executes by exploiting WinRAR remote code execution vulnerability (CVE-2023-40477) on victim's system. The exploitation may result in attacks such as ransomware, data extraction and data wiping etc.

2. Above in view, users are advised for following:

a. Do not open and download any suspicious email attachment especially password protected WinRAR/WinZip files.

b. WinRAR users are advised to update to latest version 6.23 or above.

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

- 100 -

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II)

Islamabad, the 8 September, 2023

Subject: - **Cyber Security Advisory – Prevention Against Financial Scam Activities - Impersonation as Govt Officials (Advisory No. 53)**

Context. Recently, a substantial rise in banking/financial scams has been observed using **phishing**[1], **smishing**[2] and **vishing**[3] techniques. The scammers introduce themselves as Govt Officials (FIA, SBP and Defence Force using fake official landline numbers and logos on WhatsApp DP) through call-cloning services. Resultantly, online-banking users continuously fall prey primarily due to lack of cyber security awareness, as well as advanced social engineering tactics used by scammers (call cloning, malicious apps and fake websites). As a result, malicious actors deceitfully withdraw money from user's accounts

2. **Scammers Working Model**. Financial scammers make use of the following attack vectors to exploit victim's bank account:

a. **Fake Websites – Reference of Army Poverty Alleviation Campaign**. Scammers are using spoofed websites appearing to be State Bank of Pakistan legitimate verification website and asking victims to upload personal financial details on website in reference to Pakistan Army Poverty alleviation and Revival of Economy Campaign. Fake website of State Bank of Pakistan for verification being referred is **(www.statebankverificaiton.wixsite.com)**

b. **Social Engineering**. Malicious actors masquerade phone numbers or call from unknown mobile phone/compromised WhatsApp number, masked banking official number to the victim acting as a bank employee/manager and ask for personally identifiable information (PII) like internet banking username, CNIC

[1] Phishing is fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

[2] Smishing is fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

[3] Vishing is fraudulent practice of making phone calls or leaving voice messages purporting to be from reputable companies in order to induce individuals to reveal personal information.

01

number, debit card number and debit card pin. After that the malicious actor tactfully enquires the victim whether he/she has received One Time Password (OTP) from bank and asks the user to forward it to the caller directly or by clicking on a WhatsApp link. Armed with this information, malicious actor can easily compromise any bank account and transfer money to potential account or perform online shopping.

c. **Anonymity**. The attackers use secure and anonymous cyber means to conduct the operation. Due to which, backtracking is a difficult task.

3. **Recommendations**. There is no technical solution that can eradicate and detect social engineering completely; however, safe usage of mobile/computer and compliance with security guidelines is the only way forward. Above in view, cyber awareness campaigns regarding financial scams be arranged at different forums. In addition to it, following protective measures are recommended:

a. Blocking of fake website appearing to be state bank verification website **(www.statebankverificaiton.wixsite.com)**

b. Scammers are equipped with latest technology for masking official numbers of banks. Users are advised to remain vigilant and call banking helpline themselves, immediately to verify any suspicious call.

c. Never provide sensitive information over phone to anyone, especially passwords. CNIC number and Debit/Credit Card PIN as banks do not ask for such information over phone except when user calls them for activation of debit card or internet banking account.

d. Always pay attention to suspicious numbers that do not look like real mobile phone numbers. Scammers often mask their identity by using email-to-text services to avoid revealing their actual phone number.

e. Be aware of false SMS regarding lottery schemes/Benazir Income Support Program prize offers; they are all bogus.

f. Genuine SMS messages received from banks usually contain sender ID (consisting of bank's short name) instead of a phone number in sender information field.

g. All clickable links/SMS to earn money offers are counterfeit; do not fall prey to them.

h. Never trust and reply anonymous emotional SMS as these are all traps.

i. Always use multi-factor authentication (MFA) on Internet Banking Apps, WhatsApp, Social Media and Gmail accounts.

j. Always keep a strong password for email or online account and regularly change passwords to prevent hacking.

k. Always check application permissions before installation of application and install applications from Google/iPhone Play Store only.

l. Before downloading/installing apps on Android devices, review app details, number of downloads, user reviews, comments and "additional information" section.

m. Install updated, reputed and licensed antivirus, anti-malware and anti-phishing solutions on PC and mobile devices. After installation, scan the suspected device with antivirus solution to detect and clean infections.

n. Only click on URLs that clearly indicate the website domain. In case of any doubt, users can search for the organization's website directly using search engines such as Google, to ensure that the websites are legitimate.

o. In case of banking fraud, a user should launch complaint to the concerned bank through its Helpline.

4. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

<u>All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments</u>

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 8 September, 2023

Subject: - **Cyber Security Advisory-Secure Email Communications (Advisory No. 54)**

Recently, it has been observed that hostile intelligence agencies (HIAs) have launched new sophisticated social engineering/phishing email techniques to target key civil and military officials both inland and abroad. The malicious emails appear legitimate as they contain name and appointment of genuine office-holder from civil Govt and military setups. Resultantly, the users are honey-trapped. Furthermore, non-adherence to best cyber security/secure email practices by the end users is also contributing towards the same. Numerous potential exploits such as weak passwords, unencrypted confidential correspondence sharing with vendors and sharing of classified documents through social media apps (WhatsApp etc). Use of insecure means and media to share documents is also prone to man-in-the-middle cyber-attacks and interception by HIAs.

2. Above in view, it is emphasized that all email correspondence must be made through secure email services/internet. Officials of Govt and Military setups be sensitized to avoid sharing and seeking sensitive information through insecure media or internet from private vendors. In this regard, few essential guidelines for secure email communications are attached at **Annex-I** for compliance.

3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

(Muhammad Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries/Divisions of the Federal Government and Chief Secretaries of the Provincial Governments

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

Annex-I

1. **Introduction**. Communication service is an important part of IT infrastructure within an organization. Though it is difficult to operate without requisite communication means as the same services may fall victim to hostile elements if related security practices like password protection on documents, use of encryption techniques, antispam and anti-phishing mechanism etc are not applied. It is recommended to follow secure communication practices proposed at para-2 to safeguard against hostile intrusions and sensitive data leakage.

2. **Recommendation for Email Security**

a. **Use Strong Passwords**

(1) To ensure phone security, always use strong passwords by employing combination of alphanumeric, special characters, upper- and lower-case letters.

(2) Avoid using general and easily guessable passwords e.g. date of births, own/family names, vehicle registration numbers etc.

(3) Regularly change password.

b. **Avoid Email ID Exposure**

(1) Avoid sharing email ID with unknown persons.

(2) Always confirm the identity of the individual to/from whom email is being sent/received

(3) Avoid providing personal details in suspicious internet campaigns.

(4) Never use official email for private communication. Always use separate email IDs for personal and official correspondence.

(5) Never configure/use official email on mobile phones.

c. **Be Aware of Phishing Attacks**

(1) Never open any attachments from unknown sources/senders.

(2) If an email seems suspicious, just ignore it; even don't try to unsubscribe it by clicking unsubscribe link as it may allow hacker to access your email data.

(3) Never open any attachment without anti-virus scan.

(4) If any suspicious email is received, immediately consult IT Administrator of your organization.

d. **Always Send Password Protected Documents**

(1) All email attachments must be encrypted with password.

(2) Password must be communicated through a separate channel such as SMS, call or WhatsApp message.

(3) Delete password from the sending channel (SMS, WhatsApp etc) once received by the receiving party.

e. **Use two Factor Authentication**

(1) In addition to strong password, also use two factor authentications e.g. OTP via call/message, password re-enter mechanism etc.

(2) Never share your one-time password (OTP) with anyone.

f. **Use Well Reputed and Licensed Anti-Virus**

(1) Endpoint (computer system or laptop) on which official email/data is being accessed/sent must be secured through reputed, licensed and updated antivirus/anti-malware solution.

(2) Always keep system firewall activated and updated.

g. **Use Robust Paid Anti-Spam Filters**

(1) Use reputed spam filters.

(2) Do not rely on Google's/Yahoo's spam filters as email attackers have become much sophisticated.

h. **Avoid storing data on Cloud Storage**

(1) Never Store personal and official data on cloud storage.

(2) Avoid using online document converting tools (Word to PDF etc) with cloud-based data storage technology.

i. **Recommendations for Social Media Platforms, GSM, PDF Scanner**. Few guidelines (but not limited to) are as under:

(1) Do not share official documents via WhatsApp, telegram, messenger and other so called end-to-end encrypted messaging apps/secret chatting applications as their servers are hosted outside Pakistan.

(2) Do not use online PDF scanner apps. Only scan secret documents via official hardened scanners.

* * * * *