

No.10(6)/2016-Coord
Government of Pakistan
Ministry of Science and Technology


Islamabad, 21st November, 2022

- | | | |
|--|---|--|
| 1. The Chairman,
PCSIR, <u>Islamabad.</u> | 2. The Director General,
NIO, <u>Karachi.</u> | 3. The Director General,
PSQCA, <u>Karachi.</u> |
| 4. The Chairman,
PSF, <u>Islamabad.</u> | 5. The Rector,
CU, <u>Islamabad.</u> | 6. The Director General,
NIE, <u>Islamabad.</u> |
| 7. The Chairman,
PCST, <u>Islamabad.</u> | 8. The Director General,
PNAC, <u>Islamabad.</u> | 9. The Rector,
NUST, <u>Islamabad.</u> |
| 10. The Director General,
PCRET, <u>Islamabad.</u> | 11. The Chairman,
CWHR, <u>Karachi.</u> | 12. The Chairman,
PEC, <u>Islamabad.</u> |
| 13. The Rector,
NUTECH, <u>Islamabad.</u> | 14. The Managing Director,
STEDEC, <u>Lahore.</u> | 15. The Director General,
PHA, <u>Islamabad.</u> |
| 16. The Managing Director,
NEECA, Islamabad. | | |

Subject: **CYBER SECURITY ADVISORY (ADVISORY NO.45, 46, 47, 48, 49 & 50)**

Please find enclose herewith a copy of Cabinet Division's, Cabinet Secretariat (NTISB) Letters dated 16th November, 2022 on the subject cited above for information & compliance.

Encl: As above.


(**SAEED AHMED RAHOOJO**)
Section Officer (Coord)
Tel: 9202520

Copy for information to:-

- i. PS to Secretary, MoST.
- ii. PS to Additional Secretary, MoST.
- iii. PA to Deputy Secretary (Admn), MoST.
- iv. All heads of Wing's, MoST.
- v. SO (Estt.), MoST.

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

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


Islamabad, the 16th November, 2022

Subject: - Apple Zero Day Vulnerability - iOS and iPadOS (Advisory No.45)

Apple has released a security update for zero-day vulnerability CVE-2022-42827 that allows an attacker to perform arbitrary code execution.

2. The Vulnerability affects iPhone 8 and later, iPad Pro all models, iPad Air 3rd generation and later, iPad 5th generation and iPad mini 5th generation and later. Users are advised to update devices from official app store.

3. Kindly disseminate the above message 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 Federal Government and Chief Secretaries of 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

JEA -1668
17-11-22

SECRETARY MOST
BY No. SO91
Date: 17-11-22

438/DEA-III
17/11-2022

Deputy Secretary (Admin)
By No. 2660
Date: 17-11-22

*Pl. Circulate
Compliance
Report*

By No. 222
SO (Coord)
Date: 21/11/22

DS (AD)
DEA-III
17/11/2022

JEA
17-11-22

As	
JS (Admin)	
JS (Legal)	
CFAS	
JEA	
JIA	
ISA (IS)	
ISA (Tech)	
AO (Legal)	

GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

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

Islamabad, the 16th November, 2022

Subject: - **Cyber Security Advisory – Zimbra Releases Path for Actively Exploited Vulnerability (Advisory No.46)**

Context. Zimbra has released patch for actively exploited vulnerability in its collaboration suite. The existing vulnerability could be exploited to upload arbitrary files to vulnerable instances and infect them as a web shell. As per initial estimate, around 1,600x Zimbra servers have been infected that include key organizations in government, telecommunication and IT sectors.

2. **Modus Operandi**


- a. Threat actors can weaponize existing exploits by sending an email with a crafted TAR archive attachment. The received email, along with the attachment, is submitted to Amavis which in turn uses cpio module to trigger the exploit.
- b. Various APT groups are tapping this exploit to "systematically infect all vulnerable servers." All ZCS instances using cpio are affected by this vulnerability.

3. **Patches Updates.** Patches of following Zimbra versions, along with download links are as under: -

- a. **Zimbra 9.0.0 Patch 27**
(https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P27)
- b. **Zimbra 8.8.15 Patch 34**
(https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P34)

4. **Recommendation.** Administrators of Zimbra Collaboration suite are advised to apply patches mentioned in para-3 immediately.

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


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

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of 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)

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

Islamabad, the 16th November, 2022

Subject: - **Cyber Security Advisory – Wordpress Addresses More Than A Dozen Bugs In Update (Advisory No.47)**

Context. WordPress is a widely used PHP based open source website development tool. Recently, a vulnerability (CVE-2021-25094) is identified that allows WordPress Tatsu plugin to upload a zip file without authentication. WordPress has patched this vulnerability along with other 15x security vulnerabilities (3x high severity and 12x medium/low) in version 6.0.3.

2. **Impact.** The identified vulnerabilities can allow attackers to hack websites. As per media reports, attackers have targeted around 1.4 million internet sites by exploiting the existing vulnerabilities.

3. **Updates and Patches**

- a. Web Administrators are advised to perform regular maintenance by updating latest plugins and installing security patches.
- b. Administrators must also update to Tatsu's Builder version 3.3.13.

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



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

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of 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)

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

Islamabad, the 16 November, 2022

Subject: - Cyber Security Advisory – Apache Vulnerability (Advisory No.48)


Context. Recently, a vulnerability (CVE-2022-42889) in Apache Commons Text Library is identified that can be exploited to execute remote code on servers. Apache has released a patch to fix existing Commons Text Library vulnerability.

2. **Modus Operandi**

- a. Apache Commons Text Library is an open source Java library with Interpolation system that allows developers to modify, decode, generate and convert strings into base 64 value and vice versa.
- b. After successful exploitation of said vulnerability, an attacker can perform arbitrary remote code execution to get access to the servers remotely.

3. **Patch Updates.** Administrators and users of Apache Commons Text Library are advised to update Apache to the latest version 1.10.0 immediately.

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


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

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of 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)

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

Islamabad, the 16 November, 2022

Subject: - Cyber Security Advisory – Prevention against Espionage via Typosquatting Attacks (Advisory No.49)

Context. It has been observed that cyber actors are using malicious websites with names similar to the names of legitimate government websites. The fake websites' names comprises of common misspellings or short-names of government websites (called typosquatting attack) to deceive users to unwittingly download files hosted on malicious link. Downloading and executing such files will compromise endpoint leading to attacker gaining access to system.

2. **Analysis**

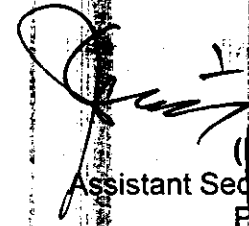
- a. **Attack Vector.** Social Engineering via emails to download malicious files from legitimate looking NTC website.
- b. **Download Link.** <http://finance.gov.pk.ntc-gov.com>
- c. **File Name.** File (circular_29092022.iso) is related to "Circulars" or "Notifications" dispatched to government setups regarding deduction of 2x day salary for flood relief victims.
- d. **Package Details.** Malicious ".iso" files further contains following 3x additional files:-
 - (1) circular_29092022.pdf (Circular for flood relief)
 - (2) circular_29092022.pdf.lnk (link [LNK] file to execute malicious payload NisSrv.exe).
 - (3) NisSrv.exe (Malicious payload).
- e. **Botnet/C&C Communication.** Following IPs are used for bot/C&C communication: -
 - (1) 51.210.32.103 (France).
 - (2) 54.145.6.146 (USA).
- f. **Malware Capabilities**
 - (1) Ability to download additional payloads.
 - (2) Bypass User Access Control with legitimate windows utilities like cmd.exe, powershell.exe etc.
 - (3) Upload files and stored usernames/passwords to C&C server.

3.

4. **Recommendations**

- a. Regularly update antiviruses such as Kaspersky, Avira, Avast etc and scan system regularly.
- b. Update all software including Windows OS, Microsoft Office and all other on regular basis.
- c. Uninstall all not in use applications and software from system and personal phones.
- d. Do not download attachments from emails unless you are sure about the source.
- e. Open Source tools and scripts such as **dnstwist** (<https://github.com/eleceef/dnstwist>) must be regularly used to **enumerate possible malicious domains** aiming at a typosquatting attack. Such domains (once found) must be **blocked** through PTA.
- f. **Awareness campaigns** be carried out by all organizations/departments to **educate their officials** about such attacks.

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



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

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of 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)

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

Islamabad, the 16th November, 2022

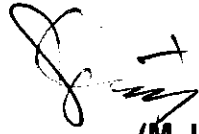
Subject: - **Advisory - Cyber Security for National Integrated Dashboard (NID) being Developed by Ministry of Planning Development & Special Initiatives and Pakistan Bureau of statistics (PBS) (Advisory No.50)**

It has been learnt that Ministry of Planning, Development and Special Initiatives/Pakistan Bureau of Statistics is developing a National Integrated Dashboard (NID) to facilitate country's top executives in decision making. NID consists of processed data of many critical stakeholders such as Ministry of Finance, Ministry of Power & Energy, SBP and FBR etc.

2. In prevalent cyber environment, cyber attacks and data compromise cannot be ruled out. It is therefore, requested that Ministry of Planning, Development & Special Initiatives/Pakistan Bureau of Statistics to perform 3rd party cyber audit of NID prior to its deployment.

3. Moreover, correspondence related to Ministries/Divisions departments should be made using secure media. Officials of Ministry of Planning, Development and Special Initiatives/Pakistan Bureau of Statistics may be sensitized to avoid sharing of sensitive information through insecure media. Guidelines for secure communications are attached at Appendix-I for compliance, please.

4. Forwarded for information/necessary action.


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

To:-

Secretary,
Ministry of Planning, Development and Special Initiatives,
Islamabad.

Copy to: -

1. All Secretaries of Ministries/Divisions of Federal Government and Chief Secretaries of Provincial Governments.
2. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
3. Secretary to the President, Aiwan-e-Sadar, Islamabad
4. Cabinet Secretary, Cabinet Division, Islamabad
5. Additional Secretary-III, Cabinet Division, Islamabad
6. Director General (Tech), Dte Gen, ISI Islamabad
7. Director (IT), Cabinet Division, Islamabad

GUIDELINES FOR EMAIL SECURITY

1. **Introduction.** Email service (e.g., Yahoo, Gmail or an organization's own email server) is an important part of IT infrastructure. Though it is difficult to operate without operational email service, but, email service may fall victim to hostile elements if pertinent security practices like password protection on documents, use of encryption techniques, antispam and anti-phishing mechanism etc are not applied. Therefore, it is recommended to follow secure email practices proposed at para 2 & 3 to safeguard against hostile intrusions and sensitive data leakage.

2. **Recommendations for Email Users**

a. **Use Strong Passwords**

- (1) To ensure email 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. DOB, own/family names, vehicle registration number etc.
- (3) Regularly change passwords.

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 email 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 emails 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 sent 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 passwords, also use two factor authentications e.g. **OTP via call/message, password reenter 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 Firewalls activated and updated.**

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

- (1) Use reputed Spam Filters.
- (2) Do not rely on Google/Yahoo's **Spam Filters** as email attackers have become much sophisticate.

h. **Avoid Storing Data on Cloud Storage**

- (1) **Never store personal and official data** on cloud storage.
- (2) **Avoid suing online document converting tools (Word to PDF etc)** with cloud based data storage technology.

i. **General Guidelines**

- (1) **Public WiFi is more susceptible** to attack as compared to private WiFi.
- (2) **Public WiFi Administrator** might be **monitoring network traffic and data sent online** via internet packets.
- (3) **Passwords** may be stored by **network Administrator**. Therefore, avoid using public WiFi for accessing personal/official email.
- (4) **Periodically review email account security settings.**
- (5) **Regularly check and apply security updates.**

3. **Recommendations for Email Server Administrators.** Following recommendations must be followed by email server administrator: -

a. **Use of Secure SSL Certificates**

- (1) Email server should be hosted on secure domains with valid **HTTPS SSL certificate**.
- (2) **SSL certificate** can be obtained from trusted vendors like GoDaddy, GlobalSign or Verisign etc.
- (3) **Free SSL certificates** may also be obtained via certificates authorities like LetsEncrypt (letsencrypt.org) or ZeroSSL etc.

- b. **Prevention against Spamming, Spoofing and Phishing.** To restrict Spamming, Spoofing and Phishing, following steps must be implemented on email server (DNS record):-
- (1) Sender Policy Framework (SPF)
 - (2) DomainKeys Identified Mail (DKIM)
 - (3) DMARC (Domain-based Message Authentication, Reporting and Conformance)
- c. Always verify and test the domain for above configuration (**Para 3b**) by checking through online websites like **dmarcian.com** (DMARC Inspector), **dkimvalidator.com** (DKIM Validator) and **mail-tester.com** (Spam Test).
- d. If email server doesn't qualify the above test (**Para 3c**) then it shouldn't be deployed in production environment.
- e. **General Guidelines**
- (1) Regularly examine email server configurations to prevent configuration drift.
 - (2) Educate and train users on use of Advanced Encryption Standard (AES) for documents (Word, PDF, PowerPoint etc) to be shared through email.

<><><>