No. 1-5/2003/24(NTISB-II) Islamabad, the 21st November, 2023

Subject: - **Cyber Security Advisory – Apple Products Operation Triangulation Linked with CVE Patch Update (Advisory No. 65)**

Introduction. Apple has released security patches to mitigate critical vulnerability, CVE-2023-32434 (Integer overflow vulnerability). In July, 2023, Apple had fixed three CVEs linked with the Operation triangulation as follows:

a. CVE-2023-32435.

b. CVE-2023-38606.

c. CVE-2023-41990.

2. **Impact**. CVE-2023-32434 is being actively exploited by threat actors in connection with "Operation Triangulation" to execute malicious code (with kernel privileges) to gain unauthorized access of victim devices.

3. **Affected Products**. Apple iPhone, iPad and iPod running iOS version 15.7 and below are affected with the above-mentioned vulnerability and consequently patches/updated versions are available.

4. **Recommendations**. Above in view, all users are advised to ensure the following:

a. **Specific Safety Steps**

M (IR-Ops)	
M (IR-P)	
M (Cus-Ops)	
M (Cus-P)	
M (Admn/HR)	
M (IT)	✓
M (FATE)	
M (Legal)	
M (Reforms)	
M (Legal & Acc. Cus)	
M (Acc. & Audit)	
Addl. Secy (Rev.Div.)	✓
SA / SPS	

(1) All Apple users should immediately upgrade to iOS latest version (17.0.3 or above).

(2) Kaspersky Lab's online malware scanning/detection tool named as "triangle_check_tool" may be utilized to inspect suspicious Apple devices.

(3) Enable Lockdown Mode (optional; extreme protection mode) to block cyber-attack.

(4) Disable iMessage feature available in iPhones.

b. **Generic Security Steps for Apple Users**

(1) Protect devices with strong passcodes and use two factor authentications on Apple ID.

(2) Install apps from official Apple Store only to avoid malware/infection.

(3) Use anonymity-based solutions (over internet while surfing) and mask identity of key appointment holders/individuals.

(4) Always disable location from Apple devices.

(5) Subscribe to Apple's security bulletins, threat notifications and auto OS update features.

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