F. No. 1-5/2003/24(NTISB-II) Islamabad, the 5 January, 2024

Subject: - **Cyber Security Advisory – Apple Products Latest CVE Patch Updates Available (Advisory No. 69)**

**Introduction**. Apple has released security patches to mitigate critical vulnerabilities (CVE-2023-42916 & CVE-2023-42917) affecting WebKit Browser Engine.

2. **Affected Products**. CVE-2023-42916 & CVE-2023-42917 is being actively exploited by threat actors to access sensitive data and execution of arbitrary code through crafted webpages on unpatched devices.

3. **Affected Products**. Apple iPhone, iPad and iPod running iOS versions (16.7.3 or older) are affected with the above mentioned vulnerabilities and consequently patches / updated versions are available.

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

a. **Specific Safety Steps**

(1) CVE-2023-42916 & CVE-2023-42917 have been patched in iOS version 17.2. therefore, all Apple users should immediately upgrade to iOS latest version (17.2 or above) from the official Apple Store.

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

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

(1) Protect devices with strong passcodes and use two factor authentication 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.

| |
|---|
| M (IR-Ops) |
| M (IR-P) |
| M (Cus-Ops) |
| M (C...) |
| M (A...) |
| M (IT) |
| M (FAIT) |
| M (Legal) |
| M (Reform) |
| M (Legal & Acc. Cus) |
| M (Acc. & Audit) |
| Addl. Secy (Rev.Div.) |
| SA / SPS |

FBR eDox Dy.No. 1991-R. Received in Chairman's Secttt on 04 JAN 2024

(4) Always disable location from Apple devices/

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

5. **References**. Latest Cyber Security Platforms including The Hacker News, Bleeping Computer, Security Week, CSIRTs etc.

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