2021

M(I.T)

Subject: **Cyber Security Advisory - Microsoft Azure Central Database Vulnerability (Advisory No. 61)**

M(Admin/HR)

1. On 27 August 2021, Microsoft has announced that its cloud computing database **Azure Flagship Cosmos DB** is vulnerable. Any customer database hosted at Azure Central Cloud can be accessed. An advisory is attached at **Annexure-A** to sensitize all concerned who are hosting their services at Azure Cloud to adopt recommended preventive measures.

A.S(Rev. Div.)

2. Forwarded for information / dissemination to all concerned, please.

Annex-A

Cyber Security Advisory - Microsoft Azure Central Database Vulnerability (Advisory No. 61)

1. **Context.** On 27 August 2021, Microsoft has announced that its cloud computing database **Azure Flagship Cosmos DB** is vulnerable. Any customer database hosted at Azure Central Cloud can be accessed.

2. **Summary of Vulnerability**

   a. **Attack Named.** ChaosDB

   b. **Adversary.** Russian government hackers (same group that infiltrated SolarWinds) that previously stole Microsoft code.

   c. **Impact.** Impact of cloud-computing attack is more devastating as they never get publicized.

   d. The flaw in visualization tool **Jupyter Notebook** and was enabled by default in **Cosmos**.

   e. The adversary can gain access to **read, change and delete main databases** of organizations / companies.

   f. The attacker can gain access to client keys to take **control of databases**.

3. **Recommendations.** Microsoft cannot change these keys; therefore, it is advised to Azure users to create new **primary read-write key** (access key) to their databases to protect their digital assets from said vulnerability.

4. **Reporting of Suspicious Files / Emails.** Any malicious activity may be reported to this organization on the following email address for analysis and suggesting mitigation measures: -

asntisb2@cabinet.gov.pk

5. Forwarded for perusal and dissemination of information to all concerned and under command, please.