GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 31 October, 2022

Subject: - **Cyber Security Advisory – Unpatched Microsoft Exchange Server Zero-Day Under Active Exploitation (Advisory No. 43)**

Context. Two **zero-day exploits in Microsoft Exchange Server (2013, 2016** and **2019)** are being exploited by malicious actors for Remote Code Execution (**RCE**) Successful exploitation of flaws can result in access to the victim's system, drop web shells and carry out lateral movements across the compromised network.

2. **Vulnerabilities**. The vulnerabilities are as below: -

a. CVE-2022-41040 – **Server-side Request Forgery (SSRF)**.

b. CVE-2022-41082 – **RCE via PowerShell**.

3. **Technical Details**

a. Microsoft Exchange Server flaws are stringed together in an exploit chain, with SSRF enabling an adversary to remotely trigger arbitrary RCE.

b. **Obfuscated web shells** are dropped on Exchange Server using **Antsword**; an active open source cross-platform website administration tool that **supports web shell management**.

c. Attacks are being launched through a lightweight backdoor that grants persistent remote access and allows attackers to reconnect at any time for further exploitation.

d. Post-exploitation activities involve **injection of malicious DLLs**, dropping/ executing additional payloads on the infected servers using the **WMI command-line utility**.

4. **Indicators of compromise**. There is no impact on the organizations which are not using Microsoft Exchange Server or **Outlook Web App** facing the internet. In otherwise case, administrators are advised to run the following PowerShell command to scan IIS logs to check if Exchange Servers have already been compromised: -

Get-ChildItem -Recurse -Path <Path_IIS_Logs> -Filter "*.log" | Select-String -Pattern 'powershell.*autodiscover\.json.*\@.*200'.

Cont'd...P/2

5. **Mitigation**. Microsoft has not yet updated patches for said CVEs. However, as a temporary measure, it is recommended to **add a rule to block requests with indicators of compromise** using the URL Rewrite Rule module for IIS servers as mentioned below: -

a. In Autodiscover at **FrontEnd**, select tab URL Rewrite and then select Request Blocking.

b. Add string "**.*autodiscover\.json.*\@.*Powershell.***" to the URL Path.

c. For Condition input: Choose **{REQUEST_URI}**.

6. Kindly disseminate the above message to all concerned in your ministries/ divisions/ departments including 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