Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No:130 **10-03-2021**

Name: Critical Microsoft Exchange Server Remote Code Execution Vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

Threat Classification: Remote Code Execution

Affected Systems: Affects the following Microsoft Exchange Server versions:

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

Summary:

Multiple critical vulnerabilities have been reported in different versions of Microsoft Exchange Server. Attackers can exploit and chain these vulnerabilities to access on-premises Exchange servers to access email accounts, and install backdoors to maintain access to victim environments.

Severity	**Critical**
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

Recommendations:

- It is highly recommended to **scan all the Exchange Server log files** using the following official link for the reported **Indicators of Compromise** (**IoC**):
  https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/#scan-log

- It is also highly recommended to immediately update Exchange Servers to **mitigate the aforementioned vulnerabilities** by following the official Microsoft link as below:
  https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

- Microsoft has also provided **Nmap script** to discover vulnerable servers within your infrastructure and also to validate the patch and mitigation state of exposed servers on below link:
  https://github.com/microsoft/CSS-Exchange/blob/main/Security/http-vuln-cve2021-26855.nse

- It is also recommended that the Administrators may use **Microsoft Safety Scanner (MSERT.EXE)** which has latest security intelligence updates to detect and remediate the latest threats known to abuse the Exchange Server vulnerabilities.

- Always use licensed and well reputed antimalware solution and regularly obtain its latest updates with its real-time scanning capabilities enabled.

- Only use licensed software and avoid download/use of cracked and pirated software.

- In case of any incident, please report to this office.