Subject: **Advisory - Microsoft Exchange Server (2010 & Onwards) Patches (Advisory No. 18)**

1. **Context.** Microsoft has released **one-click mitigation software** that applies countermeasures to secure Microsoft Exchange Server (**versions 2010, 2013, 2016 & 2019).** Administrator s are requested to apply recommendations provided at **para3.**

2. **Details of Mitigation Software.**

   a. **Name of Tool.** Exchange On premises Mitigation Tool (EOMT).

   b. **Cyber Attack Targeted.** Proxy Logon Exchange Server.

   c. **CVE Mitigated.** CVE-2021-26855.

   d. **Post Exploitation Tool.** China Chopper (Active Server Page Extended ASPX) web shell that gives access to adversary to execute code on server.

3. **Recommendations**

   a. **Prioritize** deployment of updates to affected Exchange servers:-

      (1) Exchange Servers 2010 to be patched to **KB5000978 Mar 2 2021** update and Exchange Servers 2013,2016&2019 to be patched to **KB5000871 Mar 2 2021** update

      (2) Exchange online is not affected so it does not require patching.

      (3) Exchange 2003 and 2007 are affected. Therefore, these should be upgraded to latest versions.

      (4) Analyze exchange products logs for evidence of exploitation. This process may be automated through script available at **https://github.com / microsoft / CSSExchange / tree / main / Security.**

      (5) Scan for known Webshells on own servers for Indictors of Compromise. Healt Checker Tool form **https://github.com / dpaulson45 / HealthChecker#download** to get Exchange Server updates.

* * * * *