Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 235 **26-02-2024**

Name: Active Exploitation of Critical Exchange Server Flaw (CVE-2024-21410)

Threat Classification: Critical Vulnerability, Privilege Escalation, NTLM Relay Attack

Affected Software / Services:

- Microsoft Exchange Server

Summary:

Microsoft has confirmed active exploitation of a critical security flaw in Exchange Server, identified as CVE-2024-21410, resulting in a privilege escalation vulnerability. Attackers can target NTLM clients like Outlook, leaking credentials that are then relayed against the Exchange server. Successful exploitation allows the attacker to gain unauthorized access and perform operations on the Exchange server on the victim's behalf. The threat level is heightened by the fact that exploitation has been detected in the wild.erry Robin, previously known as a USB-borne worm, has evolved into a highly sophisticated threat.

Severity	**Critical**
Attack Vector	NTLM Relay Exploitation

© Copyright 2023, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.

Recommendations:

- Install the latest security updates provided by Microsoft, specifically addressing CVE-2024-21410 for Exchange Server.
- Ensure Extended Protection for Authentication is enabled, as Microsoft has done by default with Exchange Server 2019 Cumulative Update 14 (CU14) to mitigate this vulnerability.
- Examine and reinforce configurations, especially for NTLM clients like Outlook, to minimize vulnerability to relay attacks.
- Train users on recognizing phishing attempts and suspicious emails that could lead to NTLM relay attacks.
- Deploy advanced threat protection solutions capable of detecting and blocking sophisticated attacks.
- Ensure incident response plans are up-to-date, and staff are familiar with procedures for handling security incidents.
- Maintain heightened vigilance on network activities, especially those related to Exchange Server, and promptly investigate any anomalies.
- In case of any incident, please report to this office, through PTA CERT Portal and email.

© Copyright 2023, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, dissemination or modification of this document is strictly prohibited.