Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 160 **12-12-2022**

Name: ProxyNotShell Vulnerability

Threat Classification: Server-Side Request Forgery (SSRF), Remote Code Execution (RCE)

Affected Versions:

- Microsoft Exchange Server 2013, 2016, 2019

Summary:

ProxyNotShell attack involves the use of web shells, which are dropped onto the server by chaining together two exploits, CVE-2022–41040 & CVE-2022-41082. In CVE-2022–41040, an unauthenticated Server-Side Request Forgery (SSRF) vulnerability is exploited in the Exchange Autodiscover frontend where an arbitrary request is sent with a controlled URI and controlled data to an arbitrary backend service with LocalSystem privilege. After bypassing authentication by abusing CVE-2022-41040, an attacker exploits CVE-2022-41082, in which he may run arbitrary commands (Remote Code Execution) in vulnerable Exchange Servers. Successful exploitation of these vulnerabilities allows an attacker to insert a backdoor into Exchange servers to establish persistence.

Severity	**High**
Attack Vector	**Network**
Privileges required	**Low**

Recommendations:

- Apply the Exchange Server updates for CVE-2022-41040 and CVE-2022-41082
- In case of any incident, please report to this office, through PTA CERT Portal and email