Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 242 **12-3-2024**

Name: Critical Vulnerability in Fortinet Devices

Threat Classification: Remote Code Execution (RCE)

Affected Software / Area:

- FortiOS
- FortiProxy
- FortiSwitchManager
- FortiAnalyzer

Summary:

A critical security vulnerability, identified as CVE-2024-21762, has been found in Fortinet's FortiOS and FortiProxy secure web gateway systems. This flaw allows unauthenticated remote code execution (RCE) by exploiting an improper limitation of a pathname to a restricted directory. Approximately 150,000 devices worldwide are affected, making this a high-impact threat.

Severity	**Critical**
Attack Vector	Arbitrary Code Execution

Recommendations:

- Apply patches immediately, Fortinet suggests disabling the HTTP/HTTPS administrative interface or limiting IP access to trusted hosts as a temporary workaround. However, applying official patches is strongly recommended.

- Organizations should actively monitor for any unusual activities and apply updates promptly. Regularly check Fortinet's official advisory page for the latest information and updates.
- In case of any incident, please report to this office, through PTA CERT Portal and email.