Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 149 **11-05-2022**

Name: Critical Spring4Shell vulnerability in Spring Java framework

CVE-2022-22965

Threat Classification: Remote Code Execution

Affected Versions:

- 5.3.0 to 5.3.17
- 5.2.0 to 5.2.19
- Older, unsupported versions are also affected

Summary:

It has been reported that a vulnerability Known as" Spring4Shell" was discovered in the spring, an open source framework for the Java platform. This vulnerability allows an attacker to remotely execute malicious code. It affects Spring MVC and Spring Web Flux applications running under Java Development Kit version 9 or later. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit.

Severity	Critical
Attack Vector	Network
Privileges required	None

Recommendations:

- Please visit the website link and check mitigations for the aforementioned vulnerabilities:

  https://nvd.nist.gov/vuln/detail/CVE-2022-22965

- It is recommended to immediately upgrade to secure versions 5.3.18 or 5.2.20.
- Use trusted security solutions.
- Regularly provide Cyber security awareness training to the employees.
- Do not download attachments from emails unless they are from a trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.