From: Telstra Security Operations
To: NBN Connection <nbn@email>
Subject: P1 – Critical CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+

—
Body:
Hello NBN Connection,

At 2022-03-20T03:21:00Z , we started receiving alerts of malware attacks to your network exploiting a Spring vulnerability CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+
Desciption

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. 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. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

These are the prerequisites for the exploit:

- JDK 9 or higher
- Apache Tomcat as the Servlet container
- Packaged as WAR
- spring-webmvc or spring-webflux dependency

Affected Spring Products and Versions

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

Mitigation

Users of affected versions should apply the following mitigation: 5.3.x users should upgrade to 5.3.18+, 5.2.x users should upgrade to 5.2.20+. No other steps are necessary. There are other mitigation steps for applications that cannot upgrade to the above versions. Those are described in the early announcement blog post, listed under the Resources section. Releases that have fixed this issue include:

- Spring Framework
    - 5.3.18+
    - 5.2.20+

For any questions or issues, don’t hesitate to reach out to us.

Kind regards,
Telstra Security Operations