**From:** Telstra Security Operations

**To:** <team name> (<team email>)

**Subject:** Create Firewall Rule <additional info>

—

**Body:**

Hello <team name>,

We would like to request the creation of a firewall rule and provide you more information about the ongoing attack.

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

Type of traffic to be blocked:

Block incoming traffic on clientRequestPath /tomcatwar.jsp

Block incoming traffic with headers:

suffix=%>//

c1=Runtime

c2=<%

DNT=1

Content-Type=application/x-www-form-urlencoded

The preferred response is to update to Spring Framework **5.3.18** and **5.2.20** or greater. If you have done this, then no workarounds are necessary. However, some may be in a position where upgrading is not possible to do quickly. For that reason, we have provided some workarounds below.

* [Upgrading Tomcat](https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement" \l "upgrading-tomcat)
* [Downgrading to Java 8](https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement" \l "downgrading-to-java-8)
* [Disallowed Fields](https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement" \l "disallowed-fields)

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

Kind regards,

Telstra Security Operations