From: Telstra Security Operations  
To: Networks Team [networks@email](mailto:networks@email)  
CC: nbn Team [nbn@email](mailto:nbn@email)  
Subject: Request for Firewall Rule Creation – Mitigating Spring4Shell Exploitation Attempts

Hello Networks Team,

We request the creation of a firewall rule to block ongoing Spring4Shell (CVE-2022-22965) exploitation attempts.

**Type of Attack**  
At 03:16:34 UTC on March 20, 2022, our Security Operations Centre detected active RCE attempts exploiting Spring4Shell in Spring Framework 5.3.0. Attackers are deploying a JSP web shell (tomcatwar.jsp) on Apache Tomcat servers to execute arbitrary commands.

**Traffic to be Blocked**  
Please implement a rule to block all inbound HTTP POST requests matching:

* **URI path:** /tomcatwar.jsp
* **HTTP headers:**
  + suffix=%>//
  + c1=Runtime
  + c2=<%
  + DNT=1
* **Payload signature:** presence of the parameter

class.module.classLoader.resources.context.parent.pipeline.first.pattern

Because the attack is distributed across many IPs, this application-layer filtering is essential.

**Additional Information**

* Requests use Content-Type: application/x-www-form-urlencoded
* We recommend deploying this as a WAF rule to inspect request bodies
* Continue monitoring for any requests to /tomcatwar.jsp or similar exploit patterns

For any questions or assistance, please reach out.

Kind regards,  
Telstra Security Operations