**From:** Telstra Security Operations  
**To:** Network Team (networks@email)

**Subject:** Urgent: Request to Block Malicious Traffic Targeting Spring Framework Vulnerability

Hello Network Team,

We have detected a malicious attack targeting a known vulnerability in the Spring Framework **(CVE-2022-22965)**.The attackers are attempting to exploit this vulnerability to execute remote code on our infrastructure. To prevent further attempts, we need to block requests with the following characteristics:

1. **HTTP Headers:**
   * suffix: %>//
   * c1: Runtime
   * c2: <%
   * Content-Type: application/x-www-form-urlencoded
2. **Request Data:**
   * Patterns such as:  
     class.module.classLoader.resources.context.parent.pipeline.first.pattern=...  
     These indicate an attempt to execute commands using Runtime.getRuntime().exec.
3. **Suspicious Shell URL:**
   * Block URLs containing tomcatwar.jsp, which is used as a backdoor by attackers.

Please create the necessary firewall rules to block traffic matching these patterns immediately to mitigate any further attacks on our infrastructure.

If you have any questions or need more details, feel free to reach out.

Kind regards,  
Telstra Security Operations