**From:** Telstra Security Operations  
**To:** Networks Team (networks@email)  
**Subject:** [URGENT] Request to Implement Firewall Rule – Spring4Shell (CVE-2022-22965) Exploit Mitigation

Hello Networks Team,

We are requesting the immediate implementation of a firewall rule to mitigate an ongoing malware attack targeting our infrastructure. The attack leverages a zero-day vulnerability in the Spring Framework, identified as Spring4Shell (CVE-2022-22965), which allows remote code execution on affected systems.

T elstra Security Operations has observed a pattern of malicious requests exploiting this vulnerability, specifically targeting our externally facing services running Spring Framework version 5.3.0. We have confirmed that one such attack successfully compromised services related to NBN operations.

To assist in mitigation, please apply a firewall rule with the following specifications:

* Block HTTP requests using the POST method with the URI path "/tomcatwar.jsp"
* Block requests containing any of the following suspicious HTTP headers:
  + suffix=%>//
  + c1=Runtime
  + c2=<%
  + DNT=1
  + Content-Type=application/x-www-form-urlencoded (please evaluate feasibility based on legitimate traffic patterns)

Please note that blocking by IP address may not be effective due to the distributed nature of the attack. We recommend close monitoring of any future requests to the "/tomcatwar.jsp" path and other potentially suspicious classpath manipulation patterns.

Implementing this firewall rule will significantly reduce exposure and help safeguard our infrastructure from further compromise. For any questions or clarification, please reach out to the Telstra Security Operations team directly.

Kind regards,  
Telstra Security Operations