**From:** Telstra Security Operations

**To:** Networks Team (networks@email)

**Subject:** Create Firewall Rule - Mitigating Spring4Shell Exploit

—

**Body:**

Hello Networks Team,

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

**Type of Attack:**  
We have detected an active **Spring4Shell vulnerability exploit** targeting our **NBN Connection (nbn.external.network)** service. The attackers are sending POST requests to /tomcatwar.jsp with malicious payloads that attempt **remote code execution (RCE)**.

**Traffic to be Blocked:**

* **Block all** POST **requests to** /tomcatwar.jsp unless explicitly required for functionality.
* **Inspect request bodies for** class.module.classLoader.resources.context.parent.pipeline.firstPattern and block matching requests.
* **Monitor and filter anomalous** User-Agent **headers** associated with bot-driven attacks.

**Additional Information:**  
Spring4Shell allows attackers to exploit class loader manipulation in Java applications, leading to arbitrary code execution. These rules should help contain the attack while we further investigate.

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

Kind regards,

Telstra Security Operations