**From:** Telstra Security Operations

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

**Subject:** Create Firewall Rule to Mitigate Spring4Shell Attack

—

**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:

Our analysis of the firewall logs indicates a Spring4Shell (CVE-2022-22965) malware attack targeting the NBN Connection service. The attack involves multiple POST requests to /tomcatwar.jsp with malicious payloads designed to exploit the Spring Framework vulnerability.

Characteristics to Block:

• Request Path: /tomcatwar.jsp

• HTTP Method: POST

• Specific Payload Patterns: Requests containing parameters such as class.module.classLoader.resources.context.parent.pipeline.first.pattern and related malicious payloads.

Request:

Please implement a firewall rule to block incoming POST requests to the /tomcatwar.jsp endpoint and inspect for the presence of the aforementioned malicious payload patterns in the request data. This should help mitigate the distributed nature of the attack by targeting the specific exploit characteristics rather than individual IP addresses.

Additional Information:

The attack has been distributed across multiple IP addresses within the AU region. Blocking the specific request patterns will provide a more effective mitigation strategy. Attached is a proof of concept payload that demonstrates how the attacker scripts this attack, which may aid in refining the firewall rules.

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

Kind regards,

Telstra Security Operations