**From:** Telstra Security Operations

**To:** Security Management Team

**Subject:** Create Firewall Rule

—

**Body:**

Hello

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

A suspicious activity targeting our web application layer was detected and blocked. An attempt was made to exploit the known Spring4Shell vulnerability via crafted POST requests to our Tomcat server.

Key Details:

- Source IP: [Insert IP]

- Attempted Payload: JSP Web Shell Upload

- Time of Attempt: 2022-03-20 03:16:34 UTC

- Outcome: Blocked by Web Application Firewall (WAF)

Recommended Actions:

1. Confirm that all servers are updated with the latest Spring/Tomcat patches.

2. Review server logs and file systems for unauthorized .jsp files.

3. Monitor for further attempts or lateral movement.

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

Kind regards,

Telstra Security Operations