

From: Telstra Security Operations
To: Networks Team (networks@email)
Subject: Create Firewall Rule for Spring4Shell Vulnerability

Hello Networks Team,

We would like to request the creation of a firewall rule to mitigate an ongoing Spring4Shell vulnerability exploit attempt.

We've detected multiple POST requests targeting `/tomcatwar.jsp` with payloads attempting to access the `ClassLoader`. These requests are characteristic of Spring4Shell exploitation attempts.

Please create a rule to block POST requests to `*.jsp` URLs containing the string `"class.module.classLoader"` in the request body. This should help mitigate the current attack without impacting legitimate traffic.

Additional information:

- All detected attempts originate from Australia
- The attacks target the `nbn.external.network` host

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

Kind regards,
Telstra Security Operations