**From:** Telstra Security Operations

**To:** nbn team (nbn@email)

**Subject:** Create Firewall Rule for Blocking the spring4shell vulnerability in nbn.external.network.

—

**Body:**

Hello Network Team,

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

We are currently witnessing bypasses of RCE on the nbn.external.network due to the spring4shell vulnerability in spring MVC. The specific exploit requires the application to run on Tomcat as a WAR deployment.

I would like you to create a firewall rule in the network that would block any HTTP requests directed at tomcatwar.jsp and containing payload with specific words among class.module.classLoader.resources.context.parent.pipeline.first.

Also block suspicious HTTP headers with content like below:

* suffix: %>//
* C1: Runtime
* C2: <%
* DNT: 1
* Content-Type: application/x-www-form-urlencoded

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

Kind regards,

Telstra Security Operations