**From:** Telstra Security Operations

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

**Subject:** URGENT - Create Firewall Rule – Mitigate Malware Attack

—

**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:

Remote Code Execution (RCE) or zero-day vulnerability in Spring-Core, which is caused by the Spring4Shell vulnerability. This vulnerability can be exploited by sending a malicious HTTP POST request to a vulnerable URL, which will then create a JSP shell file on the server and return the URL of the shell. The attacker can then access the shell by sending an HTTP GET request to the URL with the correct parameters.

Firewall rule:

- Block incoming traffic on client request path “/tomcatwar.jsp”

- Block incoming traffic with HTTP headers:

“

suffix=%>//

c1=Runtime

c2=<%

DNT=1

Content-Type=application/x-www-form-urlencoded

“

Additional information:

- It seems that the attack was directed at our external infrastructure using the Spring Framework 5.3.0. We should keep an eye out for any future requests to this path.

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

Kind regards,

Telstra Security Operations