From: Telstra Security Operations
To: Networks Team <networks@email>
CC: nbn Team <nbn@email>
Subject: Request for Firewall Rule Creation – Mitigating Spring4Shell Exploitation Attempts

Body:

Hello Networks Team,

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

Type of Attack

At **2:16:34 PM AEDT on March 20, 2022**, Telstra Security Operations detected an active **Remote Code Execution (RCE) attack** exploiting **Spring4Shell (CVE-2022-22965)** in the Spring Framework. This zero-day vulnerability is being used to deploy a web shell on **Apache Tomcat servers running Spring Framework 5.3.0**, allowing attackers to execute arbitrary commands remotely.

Firewall logs indicate a high volume of **malicious POST requests** targeting '/tomcatwar.jsp', attempting to inject Java code via class loader manipulation. These requests are being distributed across multiple attacker-controlled IP addresses, making traditional IP-based blocking ineffective.

Traffic to be Blocked

To mitigate this attack, we request blocking traffic with the following characteristics:

- **Block incoming traffic on client request path:** "/tomcatwar.jsp"
- **Block incoming traffic with HTTP headers:**
  - suffix=%>//
  - c1=Runtime
  - c2=<%
  - DNT=1

Since the attack is **distributed**, implementing a **Web Application Firewall (WAF) rule** to detect and block these payloads at the application layer would be the most effective response.

Additional Information

- The attack appears to be targeted at our external-facing infrastructure using Spring Framework 5.3.0.

- We recommend continuous monitoring for future requests to /tomcatwar.jsp and similar attack patterns to detect further exploitation attempts.

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

Kind regards,
Telstra Security Operations