

**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:

The Spring Framework was exploited to allow remote code execution (RCE) via data binding on JDK 9+. Specifically, this exploit requires the application to run on Tomcat as a WAR deployment.

Firewall Rule Recommendation:

We recommend adding a firewall rule to block all incoming traffic that uses /tomcatwar.jsp as a clientRequestPath.

See CVE-2022-22965 for more information on this vulnerability as well as any extra mitigation steps that the team can implement.

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

Kind regards,  
Telstra Security Operations