**From:** Telstra Security Operations

**To:** nbn team nbn@email

**Subject:** Create Firewall Rule to Prevent RCE on directory /tomcatwar.jsp

—

**Body:**

Hello nbn team,

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

This is an RCE attack. This attack is done on the directory /tomcatwar.jsp. The remote check triggers against any discovered HTTP(S) services and attempts to send a payload to common Spring-based web application paths in order to trigger an HTTP 500 response, which indicates a higher probability that the system is exploitable.   
**Block the following http header**

suffix=%>//  
c1=Runtime  
c2=<%  
DNT=1  
Content-Type=application/x-www-form-urlencoded

The affected directory is /tomcatwar.jsp, so make sure to limit access to this directory.

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

Kind regards,

Telstra Security Operations