**From:** Telstra Security Operations

**To:** Network Infrastructure Team (networking@company.com)

**Subject:** Create Firewall Rule - Spring4Shell Mitigation

—

**Body:**

Hello Network Infrastructure Team,

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

The attack leverages the Spring4Shell (CVE-2022-22965) vulnerability, using malicious HTTP POST/GET requests with form parameters designed to overwrite internal Java class loader attributes and drop .jsp web shells. The attack seems to be distributed, but request patterns are highly identifiable.

Please block or alert on requests containing any of the following keywords in URLs or POST body:  
class.module.classLoader

pipeline.first.pattern

pipeline.first.suffix=.jsp

pipeline.first.directory

pipeline.first.prefix

pipeline.first.fileDateFormat

Consider flagging requests with blank or automation tool User-Agents and high-frequency access to .jsp endpoints. This behaviour is consistent with automated exploitation scripts targeting Spring Boot apps hosted on Apache Tomcat

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

Kind regards,

Telstra Security Operations