**From:** Telstra Security Operations

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

**Subject:** [CRITICAL] Create Firewall Rule: Zero-Day Vulnerability Exploited - Action Required

**Body:**

Hello Networks Team,

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

**Type of Attack:**

The attack exploits the Spring4Shell vulnerability, allowing Remote Code Execution (RCE) on vulnerable servers.

**Attack Vector:** POST requests to "/tomcatwar.jsp"

**Payload:** Utilizes the following parameters in the POST request payload:

class.module.classLoader.resources.context.parent.pipeline.first.pattern

class.module.classLoader.resources.context.parent.pipeline.first.suffix

class.module.classLoader.resources.context.parent.pipeline.first.directory

class.module.classLoader.resources.context.parent.pipeline.first.prefix

class.module.classLoader.resources.context.parent.pipeline.first.fileDateFormat

**Additional parameters:** pwd and cmd for command execution

**Request for Firewall Rule:**

We kindly request the creation of a firewall rule to block traffic with the following characteristics:

**HTTP Method:** POST

**Path:** "/tomcatwar.jsp"

**Additional Information:**

We have observed multiple instances of this attack originating from different attacker IP addresses. The payload includes crafted parameters designed to exploit the Spring4Shell vulnerability and gain unauthorized access to the target system.

**Recommendation:**

Implementing a firewall rule to block the specified traffic will help mitigate the risk associated with the Spring4Shell vulnerability.

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

Kind regards,

Telstra Security Operations