**From:** Telstra Security Operations

**To:** NBN Team (nbn@email)

**Subject:** Create Firewall Rule <additional info>

—

Hello NBN Team,

In response to the previously mentioned attack exploiting vulnerabilities of the Spring Framework and after detailed analysis we would like to request and recommend the creation of a firewall rule to prevent escalation.

Below is a summary of our findings about the ongoing attack:

- **Type of attack:** vulnerability exploitation of Spring Framework

- **Exploit indicators**: the [ **clientRequestData** ] field contains exploitation attempts abusing [ **class.module.classLoader.resources.context.parent.pipeline** ] properties

- **Payload** also contains parameters (**pwd**) to execute arbitrary commands on the server

- **Malicious file:** [ **tomcatwar.jsp** ]

- **Source Ips (range)**: **attacker.ip.address.network1** to **attacker.ip.address.network499**

**- Origin country: Australia**

To mitigate the attack and prevent escalation we recommend to implement the following firewall rules:

1 – **Deny HTTP request** targeting [ **/tomcatwar.jsp** ]

2 – **Add rules to detect and block** request containing;

* [ **class.module.classLoader.resources.context.parent.pipeline** ]
* parameters **pwd** in the payload

3 – **IP blocking:** (*range*) **attacker.ip.address.network1** to **attacker.ip.address.network499**

4 – **Limit access to sensitive path and Java-based endpoints/applications**

5 – review and **update all Spring Framework** to the latest patched version

If further analysis is required, don’t hesitate to contact us.

Kind regards,

Michele Filandro

SOC Analyst – SOC Center

Telstra Security Operations